Quantification of Plausibility Cross-checks in Safety Related Control System Architecture Design for Automotive Applications

Andrew Robert Williams MSc, CEng, MIET

A thesis submitted in partial fulfilment of the requirements of

Birmingham City University

for the degree of Doctor of Philosophy

March 2019

The Faculty of Computing, Engineering and the Built Environment, Birmingham City University

Abstract

When designing safety critical systems for automotive applications it is imperative that the chosen architecture can fulfil the designated safety goals. One significant aspect of this is proving architectural metrics are satisfied.

The method developed in this thesis demonstrates, very early in the design process, that a system architecture can be systematically described and analysed to show that the final architectural metric targets for functional safety will be met. The system architecture model proposed can be used to explain a very complex system to other engineers / managers in an easily understood concept diagram, specifically tailored to examine the achievable diagnostic coverage of potential failures in the electrical /electronic system.

Once the first architectural model is established, the method analyses architectural metrics in a quantified way, identifies potential weak areas and guides the designer towards additional Plausibility Cross-checks, or, in some cases, completely different architectures to improve the architectural metrics. The metrics can be calculated very quickly in comparison to the level of detail required for the final design. This permits quantified analysis of each candidate architecture allowing an informed decision to be made on which architecture to take through to the final design process. Often, multiple solutions will meet functional requirements, however, only a subset will meet functional safety requirements.

The necessity to build safety into products has always been an important aspect of overall system design. This method allows decisions based on justifiable data, early in a project timeline to influence design decisions and ensure that concepts are correct. As demonstrated through examples this is achieved with a high level of confidence.

Acknowledgements

I would like to express my thanks to my Supervisor Dr Manjit Srai for his support through my Research. Thanks also go to Dr Tim Leverton for approving my request to undertake the research, Dr Roger Brassington for continually asking me whether the Thesis was finished and finally my family for their patience.

Contents

Figures

Tables

Abbreviations

AAAM	Association for the Advancement of Automotive Medicine
AADL	Architecture Analysis and Design Language
AFE	Analogue Front End
AFMDh	All Failure Modes Detected-high
AFMDl	All Failure Modes Detected-low
AFMDm	All Failure Modes Detected-medium
AIS	Abbreviated Injury Scale
ALARP	As Low As Reasonably Practicable
AMT	Automated Manual Transmission
ATU	number of Available Techniques Used
AUTOSAR	Automotive Open System Architecture
BIST	Built in Self-Test
BMS	Battery Management System
BSI	British Standards Organisation
CAN	Controller Area Network
CCF	Common Cause Failure
CRC	Cyclic Redundancy Check
CT	Confidence Table
DC	Diagnostic Coverage
DIA	Development Interface Agreement
DTC	Diagnostic Trouble Code
EASA	European Aviation Safety Agency
EAST-ADL	Electronics Architecture & Software Technology - Architecture Description Language
ECU	Electronic Control Unit
EE	Electrical / Electronic
EFMC	Element Failure Mode Contribution
FCCS	Fuel Cell Control System
FCS	Fuel Cell System
FDI	Fault Detection and Fault Isolation
FDIS	Final Draft International Standard (ISO)
FFA	Functional Failure Analysis
FIT	Failure in Time
FMDC	Failure Mode Diagnostic Coverage

FMDCC	Failure Mode Diagnostic Coverage Claim
FMEA	Failure Mode and Effect Analysis
FMvSG	Failure Mode Violates Safety Goal
FTA	Fault Tree Analysis
GSN	Goal Structured Notation
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard and Operability Study
Hip-HOPS	Hierarchically Performed Hazard Origin and Propagation Studies
HSE	Health and Safety Executive (UK)
HVIL	High Voltage Interlock
IO	Analogue or Digital Inputs and Outputs
ISO	International Standards Organisation
isoSPI	Isolated SPI (from Linear technology)
I^2C	Inter-Integrated Circuit
LFM	Latent Fault Metric
LIN	Local Interconnect Network
MBSA	Model Based Safety Analysis
MBSE	Model Based Systems Engineering
MCFMDC	Maximum Claim for Failure Mode Diagnostic Coverage
MCfT	Maximum Claim for Technique
MIR	Measure Isolation Resistance
NDA	Non-Disclosure Agreement
NHTSA	National Highway Traffic Safety Administration
NTC	Negative Temperature Coefficient
ODI	Office of Defects Investigation
OEM	Original Equipment Manufacturer
PCc	Plausibility Cross-check
PCcCF	PCc Confidence Factor
PCcDCC	PCc Diagnostic Coverage Claim
PTC	Positive Temperature Coefficient
PWM	Pulse Width Modulation
R2P2	Reducing Risks, Protecting People
RAM	Random Access Memory (Volatile Memory)
RBD	Reliability Block Diagram

RESS	Rechargeable Energy Storage System
ROM	Read Only Memory (Non-volatile Memory)
SFF	Safe Fail Fraction
SPFM	Single Point Fault metric
SPI	Serial Peripheral Interface
SysML	Systems Modelling Language
TTA	Total number of Techniques Available
UML	Unified Modelling Language
UNECE	United Nations Economic Commission for Europe
Vbat	Battery Voltage - typically 12V / 24V / 48V etc.

1 Introduction

Functional safety – 'part of the overall safety that depends on a system or equipment operating correctly in response to its inputs' (BSI, 2007) has had a high profile in areas such as petrochemical plants, aircraft, and nuclear installations etc. for many years. This is driven by good practice within the industries; in turn this develops into an international standard and is ultimately incorporated into approval processes or, as is often the case, legal requirements. In general, any system that is concerned with the consequence of failure which leads to loss of life, significant property damage or damage to the environment can be defined as safety critical (Knight, 2002).

As standardisation has evolved, functional safety considerations have migrated into other industries and it is now prominent in the automotive industry. As functionality develops, such as driver assistance and dynamic stability control, safety is one of the key issues for automotive development (Findeis & Pabst, 2006). Hybrid and electric vehicles have ever increasing electronic systems; many of which are safety critical (Ward, 2011) and have unique potential failure modes. Whenever a new system is designed, or an existing system is modified or upgraded, there is a level of risk (BSI, 2011a) and to deliver a system with a tolerable level of risk (acceptable to the operator / user of the system) rigorous processes must be adhered to. As the system complexity increases, the potential for a higher random hardware failure rate and additional systematic faults exists. Vehicle manufacturers use software intensive distributed electronic control systems (Lanigan, 2011) which must be designed and proven to be safe i.e. risk has been reduced to a tolerable level. This requires a robust design process and complex system analysis techniques employed during system verification and validation.

1.1 Research Motivation

Evolutionary development of problem context, deviation analysis, risk assessment, determination of mitigation and formulation of safety requirements (Wu & Kelly, 2006) is effective in the generation of a well understood set of requirements and a viable architecture. The architecture design can apply to logical (a structural design without specific allocation to hardware or software), hardware (physical allocation of functionality to hardware components) or software (allocation of functions to software units). Safety activities are undertaken throughout the development lifecycle, however if the correct measures are not taken in a timely manner (MOD, 2011) then the entire project can be put at risk. During the design of several different systems for both off-highway vehicles and automobiles, it has been observed that having the architecture correct at the conceptual stage of the project reduces late design changes which has several associated benefits:

- Mitigates project time delays.

- Ensures costs are controlled.
- Reduces iterative design and the associated impact analysis on the safety lifecycle.

To evaluate the final hardware design of safety critical systems in the automotive sector, up to two metrics (BSI, 2011e) are quantitatively assessed depending on the required Automotive Safety Integrity Level (ASIL) for the safety goal under consideration:

- Architectural Metrics – Single Point Fault Metric (SPFM) and Latent Fault metric (LFM)
- Random Hardware Failure Rates

Of these two metrics, considerable effort has been aimed at the analysis route dealing with random hardware failures and how this contribute to violation of the safety target for the system. This extends to Model-Based safety analysis (Joshi, 2006) using the Society of Automotive Engineers (SAE) Architecture Analysis and Design Language (AADL) which includes error modelling (SAE, 2011). This allows for modelling of errors, diagnostic coverage and allows automatic generation of fault trees using suitable tools. One such tool that allows for systems to be optimised for safety criticality and cost for example is HiP-HOPS (HiP-HOPS, 2017). The fact that the system is modelled, allows iterative design analysis as the system develops and rapid analysis of the new design. However, an important aspect for the architectural design is the architectural metric that guides the system architecture to ensure all failure modes can be adequately diagnosed both in terms of single point faults and latent faults. The architectural metrics should be analysed in addition to the probabilistic metric for random hardware failures (BSI, 2011e). This requires significant detailed circuit schematic and hardware component analysis of the final design. A description language specifically aimed at embedded systems is EAST-ADL (EAST-ADL Association, 2013) which links to the AUTOSAR standard (AUTOSAR, 2016) . EAST-ADL allows for dependability and error modelling and is focussed on ISO26262 (BSI, 2011a) and allows for omission and commission failures.

Specific standards have been developed for the automotive industry. These encompass the entire development lifecycle with ten sections covering:

1. BS ISO 26262-1, Vocabulary (BSI, 2011a)
2. BS ISO 26262-2, Management of functional safety (BSI, 2011b)
3. BS ISO 26262-3, Concept phase (BSI, 2011c)
4. BS ISO 26262-4, Product development at the system level (BSI, 2011d)
5. BS ISO 26262-5, Product development at the hardware level (BSI, 2011e)
6. BS ISO 26262-6, Product development at the software level (BSI, 2011f)
7. BS ISO 26262-7, Production and operation (BSI, 2011g)

8. BS ISO 26262-8, Supporting processes (BSI, 2011h)
9. BS ISO 26262-9, ASIL-oriented and safety-oriented analysis (BSI, 2011)
10. BS ISO 26262-10, Guideline (BSI, 2012)

The above standards cover the complete product lifecycle, however the main effort on quantifying that the final design is correct is left until the later stages in the lifecycle and the calculations are performed at component level which typically requires many hundreds of components to be analysed in terms of their failure rate, failure modes and diagnostic coverage.

1.2 Risk

Techniques exist to analyse a system in terms of reliability analysis, architectural metrics, process and audit trails etc. The process is all encompassing – from the initial idea, through design, production, in service operation and finally decommissioning. Traditional techniques such as reliability analysis, for example using fault trees or Reliability Block Diagrams (RBD's) do not give a quantified route to analyse the architectural metrics in their own right.

Whenever a system is designed there is a level of risk. As the system increases in complexity, the level of risk from random hardware faults and systematic faults increases. Different risk terms are discussed in BS ISO 26262-1 (BSI, 2011a):

Risk –	combination of the probability of occurrence of harm (physical injury or damage to the health of persons) and the severity (estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation)
Residual Risk –	the risk remaining after the deployment of safety measures

The industrial standard BS EN61508 part 2 (BSI, 2010) uses a similar approach:

Risk –	combination of the probability of occurrence of harm and the severity of that harm
Residual Risk –	risk remaining after protective measures have been taken
Tolerable Risk –	risk which is accepted in a given context based on the current values of society

The industrial standards tend to look at much larger applications than the automotive standards; for example, industrial power generation plants where, should an incident occur, there is the potential

for an increase in harm; the severity of injuries and the number of casualties that can be involved. There is also a subtle difference in the use of ‘safety’ and ‘protection’ when looking at residual risk. Often in automotive systems there is a tendency to use a common electronic controller to perform a control function and this has safety measures designed into it. In industrial applications, it is common to have a control system managing the process and an independent ‘protection’ system built around it, acting in a supervisory / shutdown capacity.

1.3 Risk Reduction

The standards all aim to reduce risk in the system through:

1) Lifecycle process.
2) Hardware design.
3) Software design.

These are equally important, but the area that can have the greatest impact on the project, especially where the project delivery relies on a number of companies, departments and disciplines, is the overall system architecture, which then progresses into lower level detail design.

The specific area of interest within the development lifecycle is the architecture design initiated at of the beginning of the process. It is imperative that the system architecture is correct at the outset as the whole of the software design and hardware design is based on the architecture.

If we jump to the end of the design process and analyse the completed system in terms of hardware failure rates and diagnostic coverage (the ability for a system to diagnose single point and multi-point faults) we can determine whether our system meets the original hardware risk reduction targets required by the safety goals and their inherited integrity level.

In some cases, it may be possible to make a qualitative assessment of the proposed safe state. A safety measure may, for example, enter a safe state which limits engine torque or vehicle speed. If, during a detected failure, the torque or vehicle speed can be guaranteed to be limited to a reduced level it may be possible to reassess the hazard with a reduced severity rating or improved controllability rating (3.3.2.3) and show that the constrained operational sate offers an acceptable level of residual risk, i.e. the situation can be controlled by an average driver. If the safety measure is guaranteed (i.e. meets the original safety integrity target) it gives a high level of confidence that the risk reduction will be sufficient if the safe state can be achieved within a sufficiently short time that a hazardous situation does not develop.

In the Automotive setting, risk is assessed, processed and measured through Automotive Safety Integrity Levels (ASIL) (BSI, 2011a). The ASIL sets a number of requirements across the product lifecycle including safety management processes, hardware design, software design, production, operation and service, and decommissioning.

1.4 Research Hypothesis

Complex system architectures can be analysed and compared by quantitative methods based on architectural metric calculations at the signal level during the concept stage of product development to accurately estimate the single point and latent point fault metrics calculated for the final design.

This thesis proposes, develops and proves a method to analyse architectures at the concept stage to compare a number of different proposals and determine the most suitable, in terms of:

- Potential to achieve the safety targets.
- Simplicity across design and verification phases.
- Cost in terms of both time and componentry.

Safety is of the highest priority, as it always should be, when dealing with systems that have the potential to introduce risk to users and / or bystanders. Cost is always a key factor when looking at a system manufactured in high volumes and compromises can be made as long as they are justified. In some cases, it may be decided that the cost to reduce the risk to a tolerable level is so high that it does not justify development of the product. As technology improves this cost balance can be re-evaluated and innovative solutions sought that reduce the risk to a tolerable level at the target cost.

Complexity can have a high cost impact. Experience shows (Leveson, 2009) that simpler safety systems often have a lower component cost and are much easier to verify / validate and in turn, this drives down design cost. Complex systems always prove harder to design 'right first time', generally incur more changes as the design evolves and are inherently harder to verify and validate – this all tends towards longer development times with an associated increase in cost. Although the function may be complex, maintaining a simple safety system around the complex function can have significant benefits.

Often, if the architecture is not right-first-time, then engineering changes are made or 'safety is added' into the system to diagnose failures discovered late in the process. This tends to increase complexity and evolving designs are unlikely to deliver an optimum solution. It is likely to take another design iteration to optimise for functionality, safety and cost.

Taking a proactive approach to functional safety in terms of a measurably safe design and just as importantly, the more intangible development of a good safety culture, can significantly reduce product recalls. The National Highway Traffic Safety Administration (NHTSA) Office of Defects Investigation (ODI) 'is observing more manufacturer recalls that involve software reprogramming and other fixes to electronics systems. This is to be expected as software intensive electronics supplant more mechanical, electromechanical, and hydraulic systems' (TRB, 2012). The cost of recalls, both in terms of fixing the problem and just as importantly repairing the reputation of the brand, should not be underestimated. Even when just considering software changes, PRQA suggest that costs have a ratio 1:10:100 (PRQA, 2016) 'That is, if a defect costs one unit (for example one hour or one dollar) to fix in requirements and design, it costs 10 units to fix in system or acceptance testing and more than 100 units to fix in production. Sometimes the cost to fix a defect in production costs much more than 100 times the cost of fixing it in the requirements phase'.

Although much of the work is based around automotive applications, the method developed is generic and can be applied to other situations such as industrial control, power generation and factory machinery for example.

There are several important reasons for performing this analysis work at the concept stage:

1) If the concept is right at the start of the project, it significantly reduces the number of design iterations as the project progresses.
2) Every change that is made during the project results in time delays and increased cost. It also has the potential to introduce new risks through added complexity.
3) Often there is less detail (conceptual information only) and so the system is easier to understand by different disciplines; electrical, electronic, hydraulic, stability dynamics, service engineers, production engineers, hardware engineers, software engineers, design group managers etc. This promotes cross-discipline discussion which often identifies potential hazards and mitigation options not always identified by pure systems engineers.

2 Functional Safety and the Background to Architectural Analysis

Functional safety is defined in BS ISO 26262-1 (BSI, 2011a) as the 'absence of unreasonable risk due to hazards caused by malfunctioning behaviour of the electric and / or electronic system'. The system scope for functional safety extends from the input(s), such as physical measurements made by the system through the control function, typically an Electronic Control Unit (ECU), to the output(s) such as actuators.

Functional safety standards have been in existence for many years. Initially quite generic in their approach but over time becoming increasingly sector specific.

2.1 Functional Safety Overview

2.1.1 Functional Safety Standards

Table 1 provides a chronological overview (applicable date at first issue) of functional safety standards that pre-dated the release of BS ISO 26262. Where multiple parts exist, only the first part has been referenced for brevity. Dates refer to the original source. For example, a standard first published by the International Organization for Standardization (ISO) e.g. ISO xxx, (where 'xxx' is the standard number) then adopted as a European Norm (EN) e.g. EN ISO xxx and then issued as a British Standard (BS) e.g. BS EN ISO xxx will show the year the original ISO xxx standard was published.

For older references, the websites that show the history of the standard have been provided as many of these publications are now withdrawn from circulation.

Table 1: A Chronological List of Functional Safety Standards

Date	Standard	Title
1965	EN 60204-1	Electrical Equipment of industrial machines – Part 1: Specification for general requirements (IEC, 1965)
1990	VDE 0801	Principles for using Computers in Safety Related Systems (DIN VDE, 1990)
1991	EN 292-1	Safety of machinery – Basic concepts, general principles for design (DIN, 1991)
1992	DO-178B	Software Considerations in Airborne Systems and Equipment Certification (RTCA, 1992)
1994	DIN V 19250	Control Technology; Fundamental Safety Aspects for Measurement and Control Equipment (DIN, 1994)
1996	ISA 84.00.01	Application of Safety Instrumented Systems (SIS) for Process Industries

Date	Standard	Title
		(ISA, 1996)
1997	BS EN 954-1	Safety of Machinery – Safety related parts of control systems (BSI, 1997)
1998	IEC 61508-1	Functional safety of electrical/electronic/programmable electronic safety related systems Part1: General Requirements (IEC, 1998)
1999	EN 50126	Railway Applications – The specification and demonstration of dependability, Reliability, Availability, Maintainability and Safety (RAMS) (CENELEC, 1999)
2000	DO-254	Design Assurance Guidance for Airborne Electronic Hardware (RTCA, 2000)
2001	BS EN 50128	Railway Applications- Software for railway control and protection Systems (BSI, 2001)
2002	IEC 61513	Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems (IEC, 2001)
2003	EN 50129	Railway Applications – Safety Related Electronic Systems for signalling (BSI, 2003)
2003	IEC 61511 -1	Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements (IEC, 2003)
2005	IEC 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronics control systems (IEC, 2005)
2006	ISO 13849-1	Safety of machinery - Safety-related parts of control systems. Part 1: General principles for design (ISO, 2006)
2008	ISO 15998	Earth-moving machinery — Machine-control systems (MCS) using electronic components — Performance criteria and tests for functional safety (ISO, 2008)
2010	ISO 25119-1	Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development (ISO, 2010)
2011	ISO 26262-1	Road vehicles - Functional Safety Part 1: Vocabulary (BSI, 2011a)

In addition, legislation has also played its part in encouraging design for functional safety. One such example is the Machinery Directive (European Parliment, 2006) which is legally binding. This uses

standards such as BS EN ISO 13849 (BSI, 2015) as a route to demonstrate compliance. With a planned edition 2 release of BS ISO 26262 in 2018 (BSI, 2016) which is currently in the final draft format (FDIS) process, the scope is changing to include trucks, buses and motorcycles. There will also be a section added for the application of BS ISO 26262 to semiconductors (ISO/DIS 26262-11, 2016). This means there may be functional safety guidelines for some aspects (the drive line) of a commercial vehicle and legal requirements for functional safety on the machinery mounted onto the vehicle. Typical examples being a cement mixing lorry or a refuse truck. This adds requirement complexity at the interface between the two systems.

As detailed above there are many standards on the subject of functional safety. Standards such as BS EN ISO 13849-1 (BSI, 2015) are prescriptive in their approach to architectures, BS EN 61508-1 (BSI, 2010a) is aimed at safety shutdown systems and others, such as BS IS0 26262-2 (BSI, 2011b) targeted at automotive control systems, are more open to interpretation and design flexibility. These standards aim to reduce the level of residual risk in a product by:

1) Following a process minimises any systematic errors that may be introduced through the design process.
2) Reducing random hardware failures through appropriate choice of components.
3) Implementing an architecture that provides sufficient diagnostic coverage to detect failures and allows a system to enter and remain, in a safe state.

Following the approaches in the standards adds a considerable amount of engineering effort and process management to the product design phases and the subsequent maintenance phases after product introduction to the market. This additional effort is justified by the increase in the levels of safety achieved in a product and the consequent reduction in the amount of risk the general public is exposed to. In some cases, companies find that the process improvements result in efficiencies in the design process that reduce overall project timelines and save costs.

An important aspect is that the system being considered is correctly defined. This means that it is completely defined in terms of the requirements that must be satisfied. The requirements must be correct and unambiguous as most errors in operational software relate to requirements (Leveson, 2009).

2.1.2 A Safe Product

'Safe' (Oxford Dictionaries, 2017) means

> *'Protected from or not exposed to danger or risk'*.

When looking at who is protected in the automotive setting consideration is given to the driver, passengers, other drivers / passengers and bystanders. To prevent them from being exposed to danger, the system must be designed to reduce the level of risk to an acceptable level.

When looking at machinery, the Health and Safety Executive (HSE, 2004) summarise functional safety as 'the safety that depends on the correct function of components or systems'. When we consider an operator working on a machine in a factory (BSI, 2015) then safety tends to look at protective measures such as guarding in terms of shields or light curtains, emergency stop buttons positioned around the machine and shut down systems that put the machine into a safe state if either a malfunction is detected or a protection barrier is breached.

In the automotive environment, risk estimation is typically more complex than a factory machine, generally the system is a lot more dynamic and there is also a driver who is an integral part of the control systems.

Security is another aspect that is increasingly discussed in the automotive arena and has significant importance when looking at connected vehicles. It specifically tackles the aspects of unauthorised or malicious attacks. Security may be violated allowing changes to the system which affect safety (The IET, 2015). Security is handled through different standards but any affects that may result in safety issues are directly covered by the proposed method. Ward (Ward, 2016) discusses how security and safety can be aligned and introduces the complexity challenges related to increases in scales and diversity of electronics. This aligns with the need to ensure correct conceptual design.

2.1.3 Risk

The standards discuss reducing risk to an acceptable level. This is rather qualitative and as a guideline to interpretation the following (Table 2) from BS 18004 (BSI, 2008) can be used.

Table 2: A simple risk estimator

Likelihood of harm	Severity of harm		
	Slight harm	**Moderate harm**	**Extreme harm**
Very unlikely	Very low risk	Very low risk	High risk
Unlikely	Very low risk	Medium risk	Very high risk
Likely	Low risk	High risk	Very high risk
Very likely	Low risk	Very high risk	Very high risk

Although open to interpretation and the application of different scales to the likelihood and severity, the table still offers guidance in terms of the scale from very low risk to very high risk. In terms of where the 'acceptable level' is set, largely depends on the area of application.

BS ISO 26262-3 (BSI, 2011c) provides all the necessary classification levels. Comparing the tables allows a simple comparison to be made between very low risk and Quality Measures (QM) and Very high risk (ASIL D). It is sufficient to understand that if a hazard has a very high level of risk (ASIL D) then this is not acceptable to the general public and so the level of risk must be reduced to an acceptable (tolerable) level.

The risk for any hazard can be classified through Hazard Analysis and Risk Assessment (HARA) and a safety goal developed that describes how the risk will be mitigated, see for example BS ISO 26262 part 3 (BSI, 2011c). An appropriate industry specific standard or guideline can be applied to define a design process and measurable targets to provide the risk reduction necessary in order to achieve an acceptable level of risk. This can be seen in Figure 1, where, as an example the hazard has been analysed as ASIL 'C'. When the analysis is performed, it is likely that the risk will be reduced below the target tolerable risk to a point defined as the residual risk.

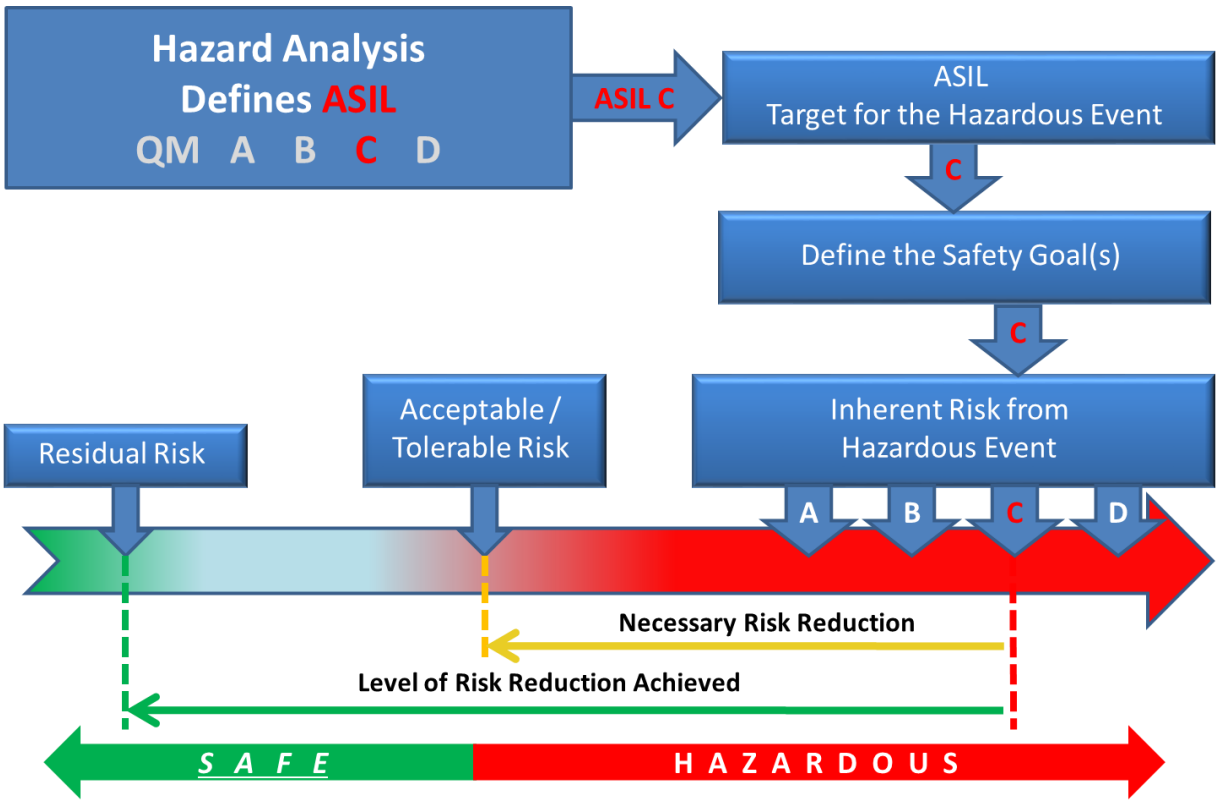


Figure 1: Risk Reduction (Adapted from Brewerton (Brewerton, 2011))

Reducing the risk lower than the tolerable risk level implies that, in practice, the design achieves a greater risk reduction than originally required. An initial assumption may be that the design is over-engineered and possibly introduces additional cost that is not required. This is a fine engineering balance and a mature life cycle process, or long product history, would be required to reduce the risk to exactly the tolerable risk target. This target is always exceeded which ultimately gives engineers a margin on the accuracy and robustness of the proof.

Risk reduction applies to each safety goal and in most designs, there will be multiple safety goals all of which must be satisfied. The design may even have conflicting safety goals, for example one safety goal may result in a design with a safe state that disconnects the battery in an Electric Vehicle. A conflicting safety goal may be to maintain torque at a level demanded by the driver. Disconnecting the battery would not allow torque to be maintained. In this example the disconnection of the battery is likely to have a higher ASIL and so take priority over the lower ASIL target. The proposed method allows the architectures to be analysed that can meet both safety goals in terms of architectural metrics. Additional work (outside of architectural metric calculations) would be required to understand if the probability of random hardware failure metrics could also be satisfied (BSI, 2011e).

2.1.4 Process Management

To deliver a safe product there are many processes that must be completed. Generally, all standards follow the standard 'V' model, an example of which can be seen in BS ISO 26262 part 1 Figure 1 (BSI, 2011b). In practice, for a complete system design there tends to be a number of smaller designs, each with their own lifecycle running in series for small projects, or in parallel for larger, more complex projects. A more realistic approach to the system lifecycle based on the authors experience can be seen in Figure 2.

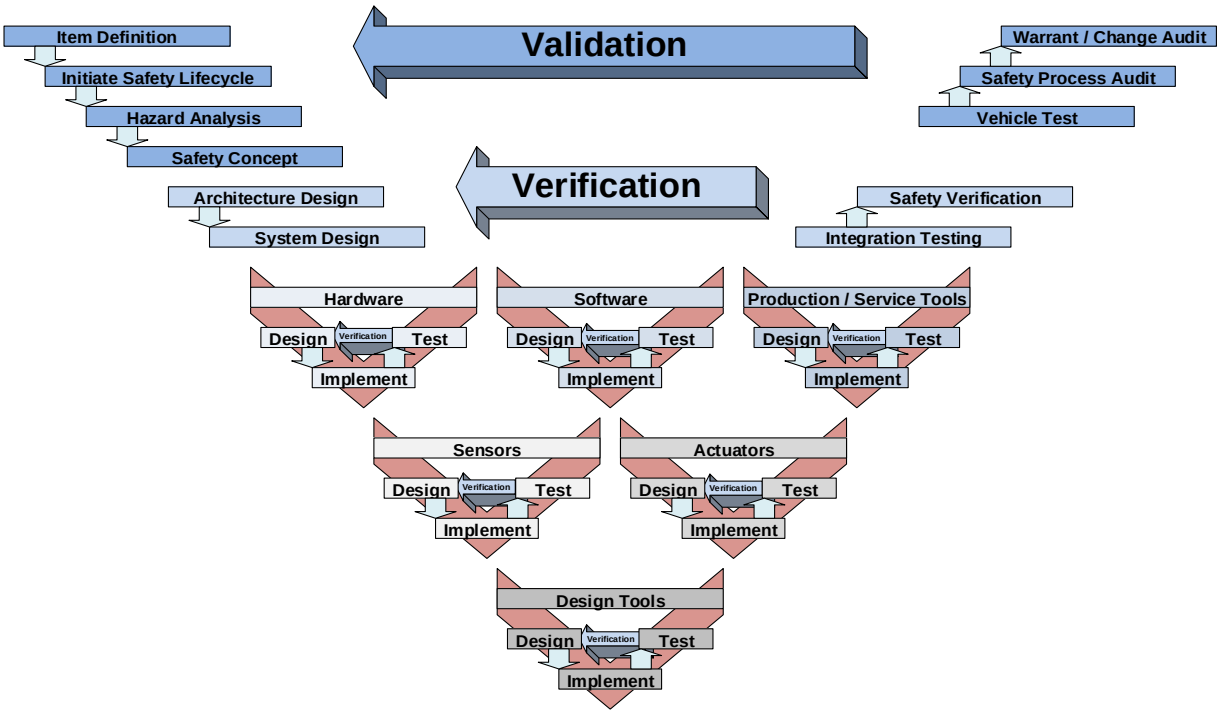


Figure 2: Practical 'V' Lifecycle Model

There are many key elements in the lifecycle which output specific work packages at each stage. These work packages provide documentary evidence that work has been completed and offer convenient points for verification and validation that tasks have been performed correctly, both in terms of engineering correctness, the level of rigour applied and process management.

Validation proves that the product meets the needs of the stakeholders at the vehicle level and verification evaluates whether the product or design meets the requirements. Typically, requirements can be defined at the system, hardware or software level and cover functional, functional safety and legislative aspects of the design.

2.1.5 Design Verification

An approach discussed by Ceunot et al (Cuenot P, 2014) uses modelling techniques to close the gap between safety design and safety verification. This looks at malfunctions and how they propagate over the architecture. The approach of function blocks for hardware architectural blocks and software functions is beneficial in describing the system but it requires a detailed level of knowledge of the system i.e. the approach requires tight coupling to the system model. Once this is known then verification can be accomplished by automated testing from the model. The approach of using a modelling approach is consistent with good design practice in that the system design is closely tied (traceable) to the final implementation.

What is required is a method to gain confidence (a quantitative analysis) earlier in the system design (at concept) that leads into the approach used by Ceunot et al (Cuenot P, 2014).

A useful example of typical development and verification processes used in the Automotive industry is given by Varadarajan et al (Varadarajan A, 2016) where a model is developed and simulated using Simulink (from Mathworks (Mathworks, 2017)) to show both typical outputs and outputs from the control system in the case of different fault injection scenarios. This is quite typical and is useful in evaluating the detection of faults in the function, but it does not offer a route to evaluation of the hardware or the level of safety integrity that can be achieved in the final design.

Lanigan et al (Lanigan P, 2010) further discuss fault injection, directly into the memory, or by manipulating data structures of an AUTOSAR (AUTOSAR, 2016) based application. For this, a running application would be required; however, at an earlier stage in verification, data over communications networks can be simulated and monitored. This provides a good basis for early testing of Plausibility Cross Checks (PCcs), possibly on a prototype ECU to prove diagnostic coverage (3.6.2) prior to having a system available for full validation. It is important to build on any lessons learned during this process as it allows PCcs to be improved and the associated requirements to be updated for use in future applications of the PCc. Once verified and validated the PCc can be re-used later ensuring continuous improvement and often improved safety integrity. The disadvantage of using a prototyping ECU is that many PCcs rely on specific hardware blocks in the microcontroller and ECU. If these are not available in the prototype ECU, confidence levels that the final implementation will achieve the same results will be reduced.

Formal methods (RTCA, 2011) can be used for verification. This requires the formalisation of the system design into a mathematical language (Cimatti A, 2010). This raises the problem that there is no precise definition of a correct requirement, but a formal approach can check that there are “no contradictions”, they are not too strict to “forbid desired behaviours” nor too weak to “allow undesired behaviours”. This level of rigour and formalisation is difficult to apply very early on with just a concept. The challenge at the concept stage is to evaluate architectures and gain confidence that when detail is added to requirements that the correct architecture is developed into a ‘correct’ set of requirements. This means that sufficient analysis has been performed to increase confidence that the system described will meet the defined item.

2.1.6 Fault Tolerance

Architectures can be defined in many ways. BS EN 61508 Part 2 (BSI, 2010) uses a method comprising of fault tolerance and safe fail fractions. Fault tolerance looks at the number of faults that can cause a loss of the safety function. BS ISO 26262 Part 5 (BSI, 2011e) looks at Single Point

Fault Metrics. Isermann et al (Isermann R, 2002) look at a fault tolerant design method. This tends to offer a system with higher levels of redundancy than those designed for automotive applications. The automotive approach for achieving functional safety adopts an additional measure referred to as Latent Fault metric that aims to ensure fault tolerance. This makes it an important attribute to consider at the concept stage of design.

2.1.7 As Low as Reasonably Practicable

In the UK, there is another principle that must be applied. This is termed 'As Low as Reasonably Practicable' (ALARP).

ALARP requires that the design is assessed to determine if risk can be reduced even further and is the way that the UK Health and Safety Executive (BSI, 2008) determines whether the risk is:

1) Very Low – risks are acceptable.
2) Low – no additional controls are necessary unless they can be implemented at low cost (in terms of time, money and effort).
3) Medium – consideration must be given as to whether the risks can be lowered, but the costs should be considered.
4) High – substantial effort should be made to reduce the risk. Considerable resources may be required to mitigate the risk.
5) Unacceptable - substantial improvements in risk control are necessary. The work activity should be halted until risk controls are implemented.

Since 1974 the HSE has produced guidelines for managing risk at work, a report, 'Reducing Risks, Protecting People' (R2P2) (HSE, 2001) refers to the use of a qualification such as ALARP. It is one of the methods employed by the UK HSE to assess any legal obligations for reducing risk. This results in good engineering practice whereby possible risk reduction is examined against the cost / trouble of implementation - which includes component cost, development cost and resource time. A judgement should be made, for example if spending £1 on a battery management system that costs £2000, can increase diagnostic coverage, allow a fault to be detected and an accident prevented which affects a few members of the public then this would need to be seriously considered and a very good justification outlined if it were not to be implemented. If, however, the only way to achieve a risk reduction was to use a triple redundant battery management system which would more than triple the cost of the product and it may only prevent a few minor accidents over the life of the product then the designers may be justified in not implementing the additional risk mitigation. Each case would have to be individually assessed on its own merits.

2.2 Model Based Design and Analysis.

Unified Modelling Language (UML) (OMG UML, 2015) is ideally targeted at software architecture design and as such does not fit exactly with the system description proposed in this method. UML, is, however very useful in understanding activities, data flows, timing and state machines when considering how plausibility checks may be incorporated in the software architecture at a later stage in the design process. To analyse plausibility checks it is necessary to simultaneously understand the possible hardware and software implementation.

The Systems Modelling Language (SysML) (OMG SysML, 2015) is dialect of the Unified Modelling Language (UML) for systems engineering applications. It is a general-purpose language used in Model Based Systems Engineering (MBSE) for modelling systems and more complex 'systems of systems' and provides analysis, design, verification and validation support. SysML offers advantages over UML and is useful earlier in the design process when understanding the overall system, i.e. before the software architecture design. The model can describe high level user interactions and the models can typically be run in a simulation mode allowing the system function and operation to be analysed, refined, and ultimately a complete set of requirements elicited. The model can be derived including malfunctions and associated diagnostics but quantifying the diagnostic capability is not possible at present. Generally, the tools 'enable you to visualize complex requirements and maintain design consistency' (IBM, 2017).

Hecht et al (Hecht, 2015) developed a method for automated generation of Failure Modes and Effect Analysis from SysML models. Although originally applied to complex aircraft systems, a similar approach can be applied to automotive systems. A relatively high perspective is taken in terms of failure modes when compared to the detailed level required for architectural metric calculations. It also concentrates on the physical elements e.g. sensors and actuators whereas the method proposed in this thesis achieves a higher level of detail by examining the signals from the sensors to the actuators and includes the intermediate logical path. The technical paper suggests next steps to address the issues of completeness of the failure behavioural models.

Sharvia and Papadopoulos (Sharvia, 2011) use Model Based Safety Analysis (MBSA), more specifically, compositional safety analysis, as a route to mitigating the problems associated with failure mode and effect analysis (FMEA) and fault tree analysis (FTA) as manual process. They also discuss disadvantages associated with performing analysis late in the lifecycle which misses the opportunity to influence early system design. This aligns with the authors thoughts on ensuring that the concept is correct, i.e. architectures are compared, and the most appropriate architecture taken through to final detailed design. The tool developed, (HiP-HOPS, 2017), Hierarchically Performed

Hazard Origin and Propagation Studies (HiP-HOPS) is a big step forward in automatic synthesis of fault trees and failure modes and effects analyses, however, at present it does not perform architectural metric calculations. This is the only tool known to decompose the system to an optimal solution. The optimal solution will depend upon the objectives set in the tool but may consider safety criticality and cost for example.

An extension to the Hip-HOPS tool has been developed by Azevedo et al (Azevedo LdS, 2014) that performs automatic ASIL decomposition. To allow decomposition within the tool it replaces the ASIL classification with simple integer algebra 'QM = 0, A = 1, B = 2, C = 3, D = 4' and uses this, along with the rules in BS ISO 26262 Part 9 clause 5.4.10 (BSI, 2011). This allows for efficient allocation of ASIL's in the most cost-effective way.

It is possible to define the model using an Architecture Description Language (EAST-ADL Association, 2013). This would allow the model to be described as per the specification but unless the complete hardware design down to component level was defined it would not allow for the specific architectural metrics for final designs to be calculated.

Mian et al (Mian, 2019) discusses the analysis of hazardous dependencies and the difficulty in detecting these in complex system. This is supported by the use of AADL and tools such as HiP-HOPS (HiP-HOPS, 2017). This is critical when considering whether failures are independent.

2.3 Reliability Analysis.

Often automotive design and development must cope with legacy elements and a pre-existing vehicle architecture (Astruc J-M, 2010). Astruc et al also discuss options based on failures of a sensor or an actuator. These can be increased reliability, failure detection within the system or redundancy. Increased reliability, although beneficial, does not contribute to diagnostic coverage and hence adds no value to the architectural metrics. The other two options discussed to increase diagnostics (redundancy through a comparison system or voting systems) are beneficial to the architectural metrics. This makes the importance of concept analysis critical and the benefits of being able to quantify different architectures even more desirable. One area not covered in the paper is common cause failures (CCF) which must be addressed when considering the system architecture. Having a single event or root cause that may result in the failure of two or more elements in the system (BSI, 2011a) must be considered when determining that elements are independent of one another.

A proposed method for software analysis (Leitner-Fischer & Leue, 2011) also has potential for hardware analysis. This proposal looks at the probabilistic method for random hardware failures but does not mention the analysis of architectural metrics. This has benefits in that a modelling method

is used with the QuantUM extension and so can theoretically be applied in a concept design but does not yet cover the architectural methods proposed in this thesis.

2.4 Re-Use and Proven in Use.

There is a tendency to reuse hardware and software in automotive applications, as in most industries, to amortise costs and increase efficiency in development / reduce time cycle to market etc. As discussed by Rupanov et al (Rupanov V, 2012), this increases re-use but limits system level analysis. To compensate for the limited analysis, new methods are proposed for systematic evaluation of design alternatives. This leads to a metamodel that includes failure modes, safety mechanisms, component details and failure effects. This approach requires a significant amount of detail and is useful at system design and hardware / software design stages but has limited application at the concept stage.

Standards, for example BS ISO 26262 part 1 (BSI, 2011a) do allow for 'Proven in Use' arguments based on previous designs, however it is difficult to collect the data in a sufficiently accurate way in the automotive setting to use this argument with confidence.

2.5 Tools for Automotive System Design

An approach specifically tailored to electrical and electronic (EE) architecture modelling is discussed by Hillenbrand et al (Hillenbrand M, 2010). This uses a layered architecture approach using a tool called PREEVision from Vector Informatik GmbH (www.Vector.com). It provides an efficient method to describe a logical architecture with traceable mapping to requirements. Since the publication of this paper, the tool has evolved considerably and now includes features such as FTA and FMEA. This requires the input of failure rate data for the analysis to be performed and is only possible once designing down to the lower levels of granularity, i.e. the hardware layer in the model. It does not offer the SPFM and LFM analysis required at the concept stage. The paper also describes the layered architecture for software as employed in the Automotive Open System Architecture model (AUTOSAR) which is described fully by the organisation that facilities this open approach (AUTOSAR, 2016). Although not directly applicable in designing a concept, the importance of aligning the concept architecture with the intended solution is very significant in structuring the overall system solution. Considering the structure of the project, which includes tools and workflows, can mitigate many integration problems later in the project, this reduces the number of changes and so improves overall safety and project efficiency. For example, knowing that the software architecture will use AUTOSAR in the final implementation (as is increasingly the preferred approach for larger automotive OEMs) leads towards a function / interface based method with a predefined tool set and workflow.

At present there are no other tools that support the Electrical / Electronic / Network full lifecycle design with built in functional safety analysis. There are other products that contribute to particular aspects of BS ISO 26262 such as Hip-HOPS discussed earlier, Mentor Safe from Mentor Graphics (Mentor Graphics, 2016), (www.mentor.com), offers a number of tools or certification documents for tools to support tool qualification and Medini Analyze from ANSYS medina Technologies AG (ANSYS medini Technologies AG, 2016) which offers a number of tool options for the safety lifecycle.

2.6 Microcontroller Options

ECUs normally contain a microcontroller for logical processing of algorithms. This highly integrated semiconductor implementation is often very complex compared to the rest of the electronics in the ECU. This means that many of the faults that occur in the system can be attributed to the microcontroller internal arithmetic units, registers, memory and peripherals. To diagnose these internal failures many diagnostic functions are required supported by internal hardware blocks. To cope with random hardware failures a typical solution in the automotive industry is to use a microcontroller based on a lockstep design. This is two identical cores running in Lockstep i.e. running identical code and the second core providing a cycle by cycle check on the main core. This is discussed in greater detail by Mariani et al (Mariani R, 2007).

Generally, the manufacturers will supply significant data to support reliability and architectural metric calculations. These calculations are only normally performed at the final design stage when all the peripherals to be used are known and the diagnostic functions have been implemented. This detailed information is normally made available under a non-disclosure agreement (NDA) by the device vendor.

2.7 Safety Perception.

Another key point is how customers perceive safety. In a survey (ELVA Consortium, 2013) it was noted that when considering electric vehicles customers were less willing to compromise on safety, interior space and cost in favour of range than they were to compromise on fast charge, climate comfort and performance. Although cost is critical to manufacturers and drives profit margins, the customer is prepared to pay for safety and it is something they are less likely to compromise; they expect the product to be safe. This report is more targeted at passive safety and advanced driver assistance systems but the fact that safety is the least likely measure to be compromised is very interesting from the functional safety engineering point of view which can often been seem as adding ‘unnecessary’ cost. To satisfy both customer and manufacturer requirements, safety is a critical aspect that must be delivered and should be as cost effective as possible i.e. designed into the product from the concept.

2.8 The Problem

There has always been a need to design a safe product and be able to prove, through supporting documentary evidence that the product is safe. The difficulty arose from trying to achieve this in a relatively small electronic engineering department with limited resource while all the time, the burden of proof increased through a desire to follow applicable guidance.

When in a large corporation designing a product with a very high volume, significant resource can be allocated to design, documentation, verification and validation as this cost can be amortised over a very large number of piece-parts and so have minimal cost implications to the cost per item.

A very small company designing low volume product may be disadvantaged by the fact that:

1) There may not be sufficient independent resource to allocate to the functional safety tasks in the same way that a much larger corporation can.
2) The product volume may be so low that the cost of implementing the functional safety process in the same way as a larger corporation may mean that the piece-part cost becomes so high that it is not worth designing it.

This really poses the problem; how to make use of the available resource to design safe products, meeting functional safety standards with the required level of integrity in the documentary evidence in a cost-effective way?

The obvious answer is to ensure that the design is 'right first time' thus ensuring that effort is only expended once rather than entering an iterative design cycle. Iterations generally invoke modifications late in the process to improve the design to the point where the safety case supports the original design targets for functional safety. However, the detailed analysis and proof can only be done once the product design is complete. It is important to remember, as discussed by Habli et al, that the argument is supported by evidence in the safety case (Habli I, 2010). This evidence gathering process can start at the concept stage and any approach that traces detection methods (plausibility checks as developed in the proposed method) from the concept through to the implementation will help to support the safety case.

Currently, architecture analysis tends to be covered by achieved failure rates. Sinha (Sinha, 2011), compares several architecture alternatives through reliability analysis. This is a valid route but relies on base failure rate data to be accurate to perform the comparison. This means that either the data must be available within the company through historic data gathering or made available by suppliers. Often suppliers are reluctant to provide this data early on in a project unless there is

confidence that the support effort involved will lead to future orders. For the comparison to be valid it also relies on different manufactures providing data that is calculated using the same assumptions to ensure a direct comparison can be made.

To date there has been little emphasis on predicting the project outcome in terms of achievable safety integrity levels related to diagnostic coverage at the beginning of the project based on quantifiable architectural metrics. The difficulty arises in having a high level of confidence that the proposed architecture will satisfy all of the design targets for architectural metrics once it has been through the design process; the method must be robust and applicable to different functional safety sectors not just automotive.

For the reliability analysis to be correct (i.e. provide the failure rate for a specific safety goal under consideration), the failure rate and failure mode distribution data for each component must be known. At the concept stage, the component selection decision is yet to be made and so this method can only be applied at the end of the design.

Even when a company has been manufacturing products for many years it can still be difficult to obtain reliability data from the field. Smith (Smith, 2005) discusses several limitations found in industrial applications such as:

1) Motivation – will a field service engineer record all relevant data if time is short?
2) Cost – failure reporting is expensive and time consuming.
3) Recording of non – failures. Has the fault been correctly diagnosed or were multiple parts changed and faults incorrectly reported when some parts were working correctly.

The work by Smith was in the context of industrial systems where components can be very expensive, and failure may cause loss of production which often enforces strict maintenance and replacement schedules. In the automotive environment correct reporting / fault analysis is even more difficult especially when customers themselves can change parts and no records are kept.

As failure rate metrics are difficult to analyse at the concept stage, it raises the question as to what other attributes are considered necessary to meet functional safety requirements that can be analysed at the concept stage.

2.9 Architectural Metrics.

One area that is critical, is the architecture of the system. A correct architecture ensures all the critical sensors, inputs, processing, outputs and actuators are able to deliver the required system

functionality. It also ensures that mechanisms exist to ensure any failures in the system can be detected and that if necessary the system can enter and maintain a safe state.

Architecture analysis using earlier references to diagnostic coverage (Smith, 2004) have, over time, been replaced by terms such as Safe Fail Fraction (SFF) (BSI, 2010a) and Single Point Fault Metric (SPFM) (BSI, 2011a) depending on the standard being used. The aim being to calculate the percentage of the sum of the safe failures and dangerous failures that are detected, as a fraction of the total number of failures. This metric allows an assessment to be made and the standards give metric targets based on the level of functional safety (risk reduction) to be achieved by the system.

BS ISO 26262 part 5 (BSI, 2011e) recommends the SPFM calculation is performed for ASIL B and is a requirement for ASIL C and ASIL D. It also recommends the LFM calculation is performed for ASIL B and ASIL C and a requirement for ASIL D.BS EN 61508 part 2 (BSI, 2010) takes a more stringent approach in that the SFF is always calculated and stipulates that the maximum SIL that can be claimed is determined by the SFF for the element and the hardware fault tolerance. This questions whether the approach in BS ISO26262 part 5 (BSI, 2011e) is sufficiently rigorous if the SPFM calculation is only required for safety goals with ASIL C and ASIL D targets. In terms of getting the design right first time and efficiently comparing architectures early in the design process then the author recommends calculation of SPFM for all safety goals at the concept stage.

BS EN ISO 13849 part 1 (BSI, 2015) relating to machinery controls also looks at diagnostic coverage. The approach (Hauke, M et al, 2008) is similar to that used in BS EN 61508 part 1 (BSI, 2010a) and BS ISO 26262 part 1 (BSI, 2011a) and is again used for self-test and monitoring but in this case refers back to the older term Diagnostic Coverage (DC). The preferred method for validation BS EN ISO 13849 part 2 (BSI, 2012) is to use a reasoned conservative estimate of the DC directly on the block or component followed by calculation of the DC_{avg} by means of an averaging formula. Estimations for Diagnostic Coverage for functions and modules are given in BS ISO 13849 part 1 Annex E (BSI, 2015)

The approach in BS EN ISO 13849 part 1 (BSI, 2015) is a more prescriptive approach where the architecture is defined based on the level of risk reduction required. This tends to work for machinery, where, typically, the safety system is a separate system to the control system. For example, it may be a switch on a finger guard or belt cover or a light curtain to prevent operators accessing moving parts of the machine. The prescriptive approach does not lend itself to more integrated systems such as automotive control systems where a more flexible approach is required to include the safety functions within the control system itself.

The reason behind the SPFM and LFM is to understand the fault coverage that has been achieved. In an automotive system, it can be argued that in terms of running a car for the average person, service and repair costs form a considerable proportion of overall lifetime costs. If all faults were correctly detected within the Electronic Control Units (ECUs), then diagnosis by service technicians would be more accurate and faster with associated reduced labour costs and increased availability for the owner. This also reduces warranty returns to OEMs and a significant reduction in 'no fault found' cases where a part has been incorrectly replaced. Faulty parts, returned with a correctly diagnosed fault leads to improved warranty data accuracy, detailed root cause analysis leads to improvement in design and it also allows failure rate data to be recorded for use in future architectural metric calculations and fault tree analysis.

Calculation of the architectural metrics have a number of benefits:

a. Improved diligence and rigour.
b. Architectural comparison of systems in a quantifiable way which may aid cost / complexity / decomposition optimisation.
c. Service diagnosis efficiency.

The author has not identified any disadvantages. Whenever this approach is taken (especially at the conceptual design phase) product improvements are identified which always advance the safety case. The effort and associated cost of doing the architectural metric calculations, even for lower ASIL targets, are eliminated in the longer term due to faster iterations during the concept stage where changes can easily be managed.

2.10 Fault Detection and Shutdown Avoidance

There are numerous ways to avoid different failures. One route is through redundant channels. This can be 2 or 3 sensors which may be identical or dissimilar (i.e. measure the system physical parameter but utilising different techniques or different manufacturers). Dissimilar sensors will increase fault tolerance as there is a lower likelihood of the same type of failure (Common Cause Failure (CCF)) affecting two or more sensors in the same way. Using a voting system on the sensors may allow the system to avoid shutdown and continue operation by relying on two sensors giving a similar value when the third is considered at fault by providing an erroneous signal.

Some techniques (Patton, 1989) utilise functionally redundant Fault Detection and Fault Isolation (FDI) to reduce reliance on redundant channels. These utilise various signal processing techniques to detect faults. This is often a cheaper solution to redundant sensors, reduces system complexity and is often employed in automotive control systems. They allow a cross check to be made between

estimated values based on other physical parameters and actual measurements. A number of the FDI techniques discussed by Patton are referenced in the standards on functional safety in terms of the types of faults that need to be detected e.g. sensor value under or over range. Different techniques can be used to improve diagnostic coverage (3.7.2.8).

Reliability and different types of redundancy are discussed by (Smith, 2005). Redundancy can be split into two different types – active and standby. Active implies that the system can function with the loss of one of the redundant channels. In standby redundancy, a failure is detected and the system switches from the failed channel to the redundant channel. In the context of high capital cost equipment, utilising redundant channels is common practice. In some cases, for example, it would allow a sensor to be removed for routine maintenance without the lost revenue associated with having to interrupt the manufacturing process.

In the automotive setting, redundant channels are much less likely even though there is an obvious commitment to safety and reliability, especially considering the volume of vehicles that are produced and the associated cost of a product recall. A more cost-effective approach is to support a limp-home mode whereby the system detects a fault and allows the vehicle to continue with reduced performance (limp-home) to allow the vehicle to be driven to a safe location for further investigation / repair. Limp-home would still be considered safe as long as the proposed system architecture can reliably detect the fault, transition to a safe mode of operation and remain in this safe mode.

2.11 Considerations when dealing with Architectural Metrics

Many factors (Lundteigen & Rausand, 2006) may influence the results of architectural metric calculations. They include increasing the safe failures by inclusion on non-essential function failures and the fact that the metrics may be calculated using different assumptions. This agrees with a note in BS ISO 26262 part 5 clause 8.5.7 (BSI, 2011e) that states that if sufficient care is not taken the architectural metrics can be biased towards components with the highest failure rates i.e. connectors and wires rather than components such as capacitors and resistors. This may require a separate analysis to ensure that the bias is not significant resulting in an incorrect result.

Both play a significant role, especially when comparing architectures. The techniques discussed later (3.7.3.1) account for these possible deficiencies in the calculations.

2.12 Methodology

From the previous discussion the methodology proposed is to maintain a close relationship to the standards to ensure that the concept calculations lead into the final analysis without modification. A

number of presentations were made at symposiums for peer review of the hypothesis. This generated an interest in the topic which later (as the method progressed) led to additional concept projects in India, Norway and the UK to examine different systems in a similar manner to the approach taken with the Fuel Cell system (4.4).

The decision was made to ensure data, where available, was collected from reputable sources i.e. component manufacturers to limit any errors between the PCc Quantification and the final design analysis. Where possible mature data 3.7.3.1 would be used as this would align concept data to the data used in the full analysis.

3 Method Proposed.

The proposed method ensures that the main verification loop shown in the Practical 'V' Lifecycle Model (Figure 2) does not become iterative due to problems discovered late in the design program. It achieves this through a much simpler, more efficient, iterative process at the Safety Concept / Architecture Design / System Design phase of Figure 2. The method and how it fits into the above lifecycle can be seen in Figure 3. The method concentrates on architectural metrics and so the final design will still have to comply with the other aspects of the applied standard (ISO26262 for example).

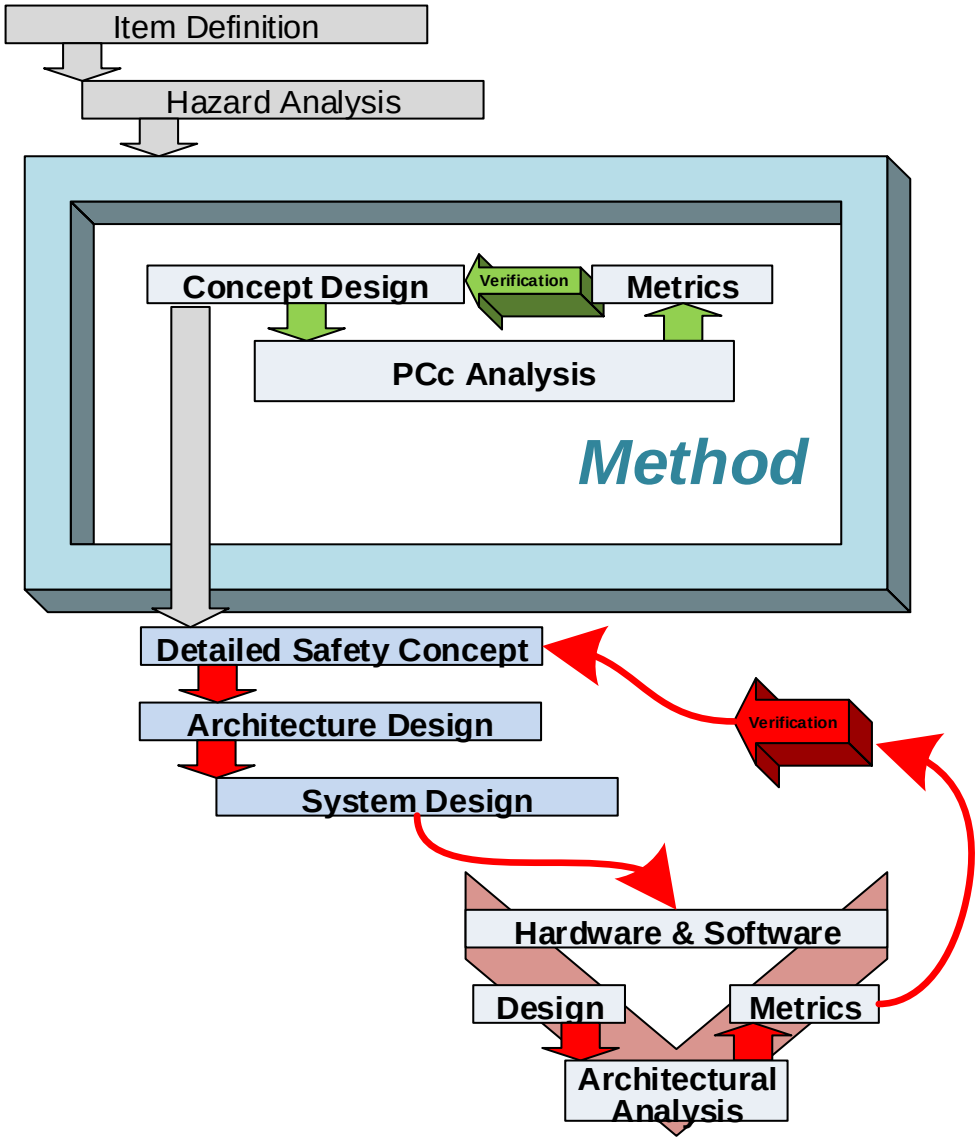


Figure 3: Area of Interest for the Proposed Method

The area of interest for the proposed method is firmly established within the concept phase. The red arrows (Figure 3) indicate the iterative process generally seen at present. The green arrows show the much tighter iteration performed in the concept stage which is designed to significantly reduce or eliminate the costlier iteration (red loop). This allows the concept to progress from basic functionality to improved concepts with better architectural metrics in a very short period. In the method, the hardware and software implementation stages are replaced with Plausibility Cross-check (PCc) Analysis, i.e. a theoretical design concentrating on architecture rather than design execution.

3.1 Introduction

To be successful, the proposed method needs to deliver four main outcomes (3.2). The method takes a number of design targets (3.3), describes the system (3.5), considers possible faults (3.6),

analyses a number of solution proposals in order to satisfy the design targets (3.7) and selects the most suitable candidate for continued development (3.8). Importantly, this is all possible at the concept stage.

3.2 Outcomes

Testing the hypothesis will generate a number of outcomes:

1) Describe a complex system, or combination of systems, in a way that can be understood by engineers from other disciplines such as hydraulic, mechanical, powertrain etc. rather than purely systems or functional safety engineers. It should also allow explanation of the system to technical managers and non-technical managers (marketing / purchasing / finance etc.).
2) Allow different architectures to be explored quickly, both at the higher system level (e.g. a vehicle) and at the sub-system level (e.g. a battery pack).
3) Provide a quantitative analysis of the proposed architectures resulting in a sound argument for the chosen candidate to take forwards through to detailed design.
4) Comparison against safety targets which must integrate easily into the required functional safety standard for the chosen discipline whether this is automotive, off-highway vehicles or industrial machinery for example.

The quantitative analysis is challenging in that the standards perform quantified analysis in diverse ways. However, effectively they all analyse the failure to meet a safety target based on the diagnostic coverage that can be obtained for each failure mode of each component that results in a violation of the safety goal. This means that the method can be applied irrespective of the applicable standard. It should be remembered that the architectural metrics are for one safety goal; typically, a number of safety goals much be satisfied for a single system and although architectural metrics can be treated for each goal individually, the overall probability of random failures calculations for one safety gaol may be affected by the inclusion of components used to satisfy architectural metrics for another safety goal.

For the purposes of this Thesis, analysis is performed as per BS ISO 26262 (BSI, 2011e) as this requires values for single point and multiple point failures to be quantified and the author has extensive experience in the automotive functional safety discipline.

3.3 Design Targets

Each of the outcomes defined in 3.2 follow on from each other. The missing element (discussed in this section) is the safety target which is required for the comparison following the quantified analysis. As this is normally the starting point to the entire process and aids in understanding the importance of functional safety it has been included for completeness. In an ideal world, the safety targets would come from the customer (OEM) as they have control over all the items being integrated to form the complete vehicle system. They also have responsibility to demonstrate compliance with the top-level vehicle safety targets i.e. the overall safety case.

3.3.1 Risk Identification

There are several different methods employed to identify risks; these include, but are not restricted to brainstorming, quality history, FMEA and Hazard and Operability (HAZOP) studies (BSI, 2016). Often, a function based approach is taken, such as a Functional Failure Analysis (FFA). At the concept stage this can be a qualitative assessment used to identify hazards. It can also be used in a quantitative manner by decomposing the functional architecture and adding functional criticality ratings (Kurtoglu T, 2010).

The European Aviation Safety Agency advises that hazard identification should be treated as a dynamic process rather than a static design (EASA, 2011). This is desirable in automotive applications and is implicit in the BS ISO 26262 approach in ensuring that 'all' hazards have been identified at the vehicle level for the system under consideration. The system will have a well defied boundary. To identify 'all' hazards typically a number of different techniques are used as discussed later.

BS ISO 26262 part 3 (BSI, 2011c) covers the HARA and includes consideration of the following areas:

1) Situation Analysis; vehicle usage scenarios such as high-speed driving, parking, reversing, off road driving, trailer towing etc.
2) Environmental conditions; ice, rain, side winds etc.
3) Reasonably foreseeable driver misuse.
4) Interaction between operational systems.

The important criteria are that the list is comprehensive and has identified all possible hazards. When determining hazards, no merit is given to any existing or planned safety mechanisms designed to mitigate the hazard. The aim is to identify all possible hazards that can occur. This may be cross referenced against a known hazard list for completeness.

Hazard identification analysis is performed at the vehicle level. This is a crucial point; it means that the wider picture must be analysed not just the specific hazards resulting from the malfunction of

one particular system / component that the company may be designing. Even though a company may be designing a generic product without a specific vehicle platform in mind which is termed 'out of context' in BS ISO 26262 (BSI, 2012) the whole vehicle must be considered. This forces the analysis to consider how other systems interact i.e. can one function / system affect another function / system. A HAZOP was conducted for an electric vehicle (refer to Appendix B – Hazard Identification) to identify all hazards at the vehicle level.

The author promotes an iterative three stage approach. Initially the item is defined and includes:

1) A list of functions without considering the input source or output destination.
2) A list in interfaces. This may be relatively difficult at the concept stage, but the basic interfaces can be defined even if exact detail is unknown. For example, an input may be 'cell voltage' but the source may be unknown and may ultimately be a hard-wired input, data from a distributed system or multiplexed through an analogue front-end converter. The important fact at the concept stage is that hazards related to the cell voltage signal can be identified. In many cases mechanical / physical interfaces are also included to ensure all hazards are identified.

In the second stage two approaches are then applied independently (separate meetings):

1) FFA (Kurtoglu T, 2010) which is applied purely to the function AND
2) HAZOP (BSI, 2016) which is applied purely to the interfaces to / from a system / function.

Thirdly the hazards are compared to a maintained and controlled Company Hazard List. This allows:

1) Any hazards that have been identified previously to be considered. These hazards may come from internal hazard identification activities or external referencing for example international databases on vehicle recalls such as that provided in the UK (VOSA, 2017) and Canada (Government of Canada - Transport Canada, 2017).
2) The Company Hazard List is updated to include any new hazards identified by analysing the item under consideration.

This offers many advantages:

1) The processes use different guide words and so impose a slightly different thinking when identifying hazards i.e. the system is examined from different viewpoints
2) The two methods can be conducted by two different teams, with a common chairperson. For example, the functional failures being analysed by a driver / user and controls

engineering based team and the interfaces by a systems integration / hardware engineering-based team.

3) The chairperson can align common hazards to ensure consistent wording for common hazards and ultimately agree the overall hazard list from the two approaches.
4) The approach is interactive. The function analysis may identify that additional inputs / outputs are required than initially defined for the item.
5) Signals may not be available within the boundary of the item which may increase system scope and identify additional interfaces required within the item.

3.3.2 Classification of Hazardous Events

The generic risk estimator (Table 2) was further evolved in BS ISO 26262 part 3 (BSI, 2011c) so that the level of risk is categorised in terms of an Automotive Safety Integrity Level (ASIL). The simple risk estimator takes no account of the driver in the control loop and how well they may be able to control the vehicle in the event of a component or system malfunction. This was addressed originally by MISRA (MISRA, 2007) as a controllability factor which adds another dimension to the risk analysis. The automotive risk analysis also terms the likelihood of harm as severity. To complete the risk analysis a number of parameters must be defined as required in BS ISO 26262 part 3 (BSI, 2011c):

1) Severity (3.3.2.1)
2) Exposure (3.3.2.2)
3) Controllability (3.3.2.3)
4) Driving / Environmental Conditions (3.3.2.4)

3.3.2.1 Severity

An estimate of the severity of harm to each endangered individual. This includes the driver, passengers, cyclists, pedestrians and occupants of other vehicles. The severity of an injury can be described by the Abbreviated Injury Scale (AIS) (AAAM, 2015) (Table 3).

The AIS Stage can be assigned to the various classes of severity. For the purposes of this work the following cross references have been used depending on the type of hazard being considered:

1) Table 4Cross reference to severity (Table 4).
2) Vehicle speed difference where a collision is under consideration (Table 5).
3) Vehicle activity where a pedestrian / cyclist injury is under consideration (Table 6).

Table 3: Abbreviated Injury Scale (AIS) (AAAM, 2015)

AIS Stage	AIS Description
AIS 0	No injuries
AIS 1	Light injuries such as skin-deep wounds, muscle pains, whiplash etc.
AIS 2	Moderate injuries such as deep flesh wounds, concussion with up to 15 minutes unconsciousness, uncomplicated long bone fractures, uncomplicated rib fractures etc.
AIS 3	Severe but not life-threatening injuries such as skull fractures without brain injury, spinal dislocation below the fourth cervical vertebra without damage to the spinal cord, more than one fractured rib without paradoxical breathing etc.
AIS 4	Severe injuries (life-threatening, survival probable) such as concussion with or without skull fractures with up to 12 hours of unconsciousness, paradoxical breathing
AIS 5	Critical injuries (life-threatening, survival uncertain) such as spinal fractures below the fourth cervical vertebra with damage to the spinal cord, intestinal tears, cardiac tears, more than 12 hours of unconsciousness including intracranial bleeding
AIS 6	Extremely critical or fatal injuries such as fractures of the cervical vertebrae above the third cervical vertebra with damage to the final cord, extremely critical open wounds of body cavities (thoracic and abdominal cavities) etc.

Table 4: AIS cross reference to severity (based on (BSI, 2011c))

Class	Description	Reference for Single Injuries
S0	No injuries	AIS 0
S1	Light and moderate injuries	>10% probability of AIS1-6 and not within S2 or S3
S2	Severe and life-threatening injuries (survival Probable)	>10% probability of AIS3-6 and not within S3
S3	Life-threatening injuries (survival uncertain), fatal injuries	>10% probability of AIS5-6

Table 5: Vehicle speed cross reference to severity (based on (BSI, 2011c))

Class	Description	Reference based on Speed △V between two vehicles
S0	No injuries	
S1	Light and moderate injuries	△V <20kph
S2	Severe and life-threatening injuries (survival Probable)	20kph<△V<40kph
S3	Life-threatening injuries (survival uncertain), fatal injuries	△V>40kph

Table 6: Pedestrian / cyclist cross reference to severity (based on (BSI, 2011c))

Class	Description	Reference based on Speed for pedestrians / cyclists
S0	No injuries	
S1	Light and moderate injuries	Parking
S2	Severe and life-threatening injuries (survival Probable)	Urban area driving i.e. 20mph in UK outside Schools when access is required or 20mph at other times
S3	Life-threatening injuries (survival uncertain), fatal injuries	Driving outside of a built-up area

3.3.2.2 Exposure

Estimate the exposure of each endangered individual. This includes the driver, passengers, cyclists, pedestrians and occupants of other vehicles. For the purposes of this work the following exposures (Table 7) have been used.

Table 7: Exposure classification (based on (BSI, 2011c))

Class	Description	Quantified Rate
E1	Very Low probability	<0.1% of operating time
E2	Low probability	<1% of operating time
E3	Medium Probability	<10% of operating time
E4	High Probability	>=10% of operating time

If operating time is not appropriate, then a frequency-based approach can be used. For example, driving in an urban environment can be classed as >10% of operating time but towing a trailer may be a few times per year (BSI, 2011c).

3.3.2.3 Controllability

Controllability is defined as the ability to avoid a specific harm or damage through the timely reactions of the persons involved BS ISO 26262 part 1 (BSI, 2011a). This term is only included in the automotive functional safety standards as the driver can be considered as part of the control loop. For example, if electric power steering assist fails then the driver can compensate and still bring the vehicle to a safe stop without endangering themselves, passengers or bystanders. In, for example, a chemical process plant it is unlikely that an operator would intervene other than using an emergency stop if the control system fails. Controllability is classified into four categories (Table 8) as based on original work by The Motor Industry Software Reliability Association (MISRA) (MISRA, 2007).

Controllability can be subjective. As Pocock et al discuss regarding trained operators, it is 'important to understand how work will *actually* be performed as opposed to how it is *envisaged* it will be performed' (Pocock, 1999). Passenger cars (unlike commercial vehicles) assume only basic training and assessment (i.e. a driving test) and so a major part of determining controllability must be based on simulation, live data – i.e. introducing faults and monitor behaviour or statistical data from previous accident analysis (NHTSA, 2008).

Table 8: Controllability Classification (based on (BSI, 2011c))

Class	Description	Definition	Examples
C0	Generally Controllable	Generally possible to control	Situations that are considered distracting
C1	Simply Controllable	99% or more drivers and other participants can avoid harm	E.g. steering column locked when pulling away. Can easily bring car to rest before achieving sufficient speed to do harm
C2	Normally controllable	90% or more drivers and other participants can avoid harm	e.g. emergency braking with ABS failure, Loss of power assist steering
C3	Difficult or uncontrollable	< 90% of drivers and other participants can avoid harm	e.g. total loss of braking

3.3.2.4 Driving / Environmental Conditions

Another key factor to consider when performing the risk analysis is the operational situation. There are many variables that can affect the vehicle state at the time that the fault occurs. These include road conditions (e.g. tarmac, concrete, rough ground) and environmental conditions (e.g. rain, snow, heat). These must be comprehensive but also address sensible limits that can be foreseen. For example, cold, hot, wet, icy conditions can be considered for most hazards. However, rough terrain can be considered for a 4x4 vehicle but not for a city car. Consideration should also be given to foreseeable misuse of the vehicle. Further information is provided in ISO26262 Part 3 (BSI, 2011c).

3.3.2.5 ASIL Determination.

Once the severity (S), exposure (E) and controllability (C) are known they can be referenced in the ASIL determination table (Table 9) to determine the ASIL (from BS ISO 26262 part 3 Table 4 (BSI, 2011c)) applicable to the hazard.

Table 9: ASIL Determination (BSI, 2011c)

ISO 26262 Risk Graph		Controllability		
Severity	**Exposure**	**C1**	**C2**	**C3**
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

For each hazard under consideration an ASIL is derived in the range QM, ASIL A, ASIL B, ASIL C or ASIL D. If the hazard has many different operational situations, the worst-case rating (highest ASIL) would be taken for the hazard.

The next stage in the design is to allocate a safety goal to each hazard; the safety goal describes how the hazard will be mitigated. Where possible this is a positive statement, for example, 'Cells shall be maintained within their safe operating envelope for voltage and temperature'. This promotes the complete system design in a positive light and is preferred goals such 'Unsafe operation of the cells shall not be tolerated' generates a negative feeling to the entire process; the start of the design informs the designers of everything they can't do as opposed to everything positive that the design needs to achieve. An additional benefit is that a positive safety goal implies designing in functional safety into the system rather than just relying on fault detection and mitigation.

Once all safety goals are defined the system can be conceptualised.

3.4 PCc Method.

An overview of the method is shown in Figure 4. It shows the stages (described in the following text) and a graphic for each of the diagrams and spreadsheets associated with each stage. Each of the graphics are shown in more detail in the following sections.

The diagram shows the relatively short iterative loop (green arrow) that is used to ensure that the required confidence is achieved in the architectural metrics required for the functional safety standard being applied to the system of interest.

At the end of the method, the engineer would continue with the detailed system design and subsequent hardware / software design or through a Development Interface Agreement (DIA) (BSI, 2011a) with a suitable competent supplier.

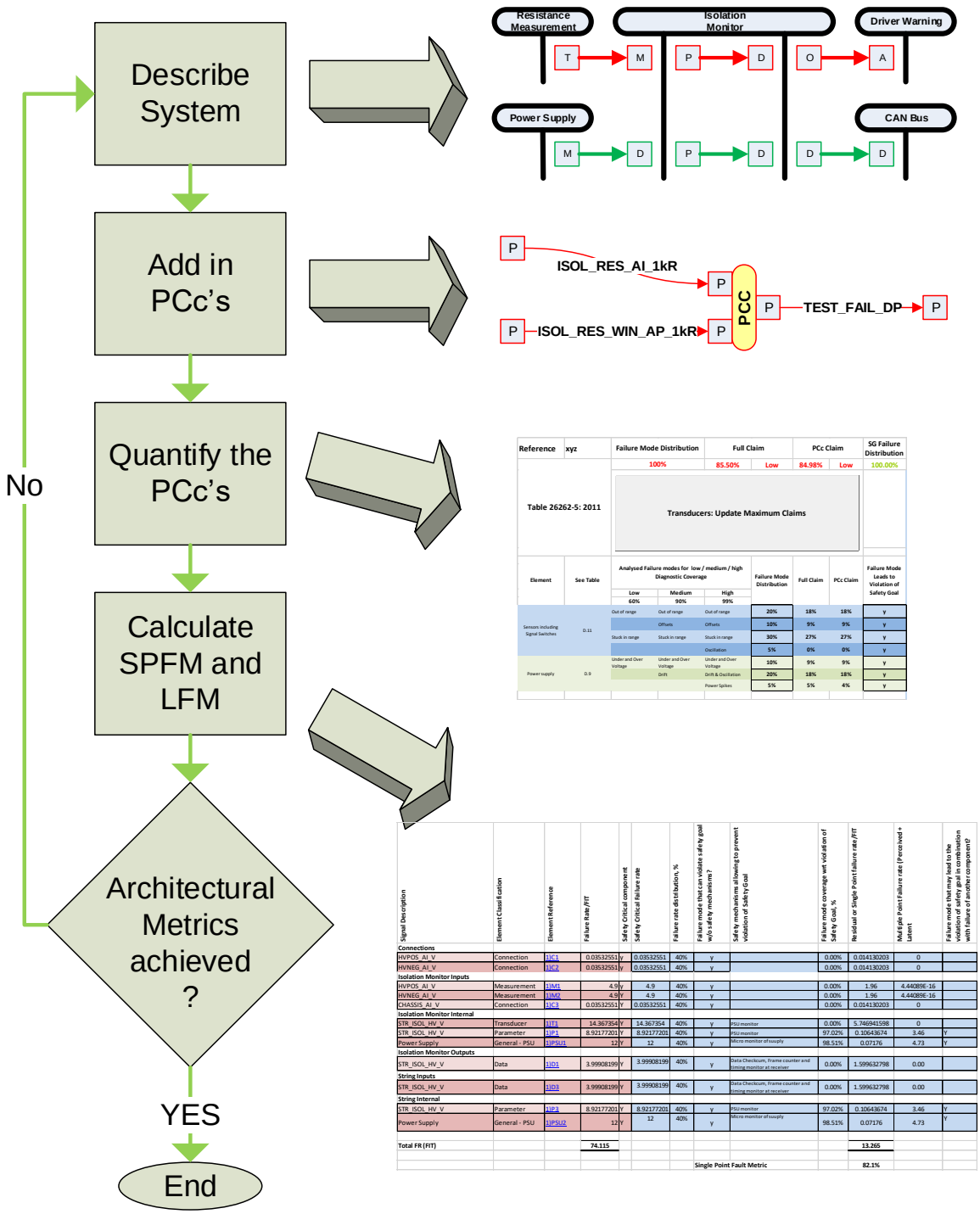


Figure 4: PCc Method

3.5 System Description

The aim of the system description part the method is to provide a graphical representation of the system using a sub-set of elements in order start the analysis process. An example of a very simple control system (Figure 5) consists of an input from a transducer, a control function (f) and an output to drive an actuator.

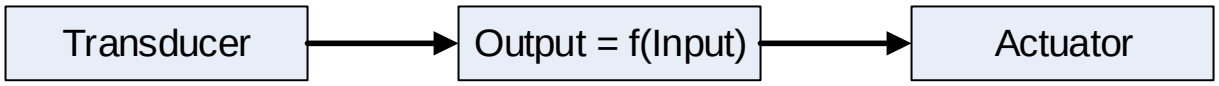


Figure 5: Simple System

Maintaining this simple approach allows the different points of connection (signals and their interfaces) to be considered. The sensor has an output connected to an input on the control system. An output from the control system connects to the input of an actuator. In terms of hard-wired connections, it is now possible to build a complex system (see Figure 19) which may have multiple inputs feeding multiple functions with multiple outputs. The method is concerned with the detection of failures at the elements classified in section 3.5.2, this doesn't classify a function as an element rather it looks at failures in terms of data or parameters at the signal level which are generated or modified by functions i.e. Output = f(Input) as in Figure 5. Signals as parameters or data may pass to multiple other functions or outputs allowing an array of systems to be analysed.

BS ISO 26262 part 5 (BSI, 2011e) defines the system as containing generic hardware components:

1) Systems.
2) Electrical Elements.
3) Processing Units.
4) Non-volatile Memory - Read Only Memory (ROM).
5) Volatile Memory - Random Access Memory (RAM).
6) Analogue and Digital Inputs and Outputs (IO).
7) Communications Bus (serial, parallel).
8) Power Supply.
9) Program Sequence Monitoring / clock.
10) Sensors.
11) Actuators.
12) Combinatorial and Sequential Logic.
13) On-Chip Communication.

The above categories, although generic, relate to components that fall into specific categories and can only really be applied later in the design process when the control system containing all of the components is defined. This causes problems when designing at the concept level as this information may not yet be known. More importantly, the achievable safety integrity level of the whole design of the system may be influenced by decisions made at this point. This enforces the 'right first time' mentality and is one of the driving forces behind this work.

The diagnostic coverage section is always detailed in the hardware section of safety standards. This is because it is trying to reduce the number of undisclosed failures and it is related to the random hardware failure rate of the components and their failure modes. Again, this is information not yet known at the concept stage. To achieve sufficiently high diagnostic coverage, effectively two things are required:

1) A detection method. Examples of feedback in hardware are a verification signal on an input that confirms a particular input value, or output that can report the status.
2) Some method of cross-checking the input to the verification signal or the output to the feedback signal.

It is rare to find a complex system that does not contain a microcontroller. This microcontroller will generally provide the necessary cross-checking through software. Software is not directly considered in the diagnostic coverage / architectural metrics calculations as a separate term. It is however used to determine the level of diagnostic coverage that can be achieved. This leads onto the idea of Plausibility Cross-checks as being a high-level method of detecting a failure that is not yet allocated to a particular hardware component or even to a specific area of the system. This allows it to be applied at the concept level.

In some cases, diagnostics may be completely designed in hardware. In this case it is still common to have a PCc performing a self-test to identify latent faults in the system.

3.5.1 System Itemisation

To analyse the system, the major building blocks need a degree of itemisation to be able to perform the analysis at the concept stage.

Some of the generic categories from BS ISO 26262 part 5 (BSI, 2011e) discussed above (3.5), are sufficiently high level to be included at the concept stage. This includes actuators, inputs and outputs. Some initially appear generic, for example a sensor. However, some sensors can be considered simple and others may be a complete system in themselves and be subject to design

guidelines such as BS ISO 26262 in their own right. For this reason, sensors were divided into two categories:

1) Voltage measurement.
2) Transducers.

The sensors can be a simple voltage measurement type or a more complex transducer converting, for example, air mass flow to a voltage signal for use in combustion control algorithms.

Considering how electrical systems are constructed on cars (equally applicable to industrial implementations) there is a need to include connectors to connect wiring harnesses from different physical entities on the vehicle together. For example, the transmission may have its own harness which is then connected to the main powertrain harness during the build process. Therefore, connectors should also be considered as part of the analysis as failures at the connection point may be significant. Care should be taken when looking at connectors and consideration given to including wires / harnesses when looking at architectural metrics. The author recommends that connectors at sensors / ECUs / actuators etc. are considered but not wires and connectors / splices in the harness. The reason being that:

1) Electrical elements tend to have relatively high failure rates compared to the more reliable electronic elements and so can bias architectural metrics towards elements with the higher failure rates.
2) If a fault at the signal interface level (as discussed in 3.5.2) to the electronic element has sufficient diagnostic coverage to achieve the architectural metrics for the inherited ASIL (highest from the allocated safety goals) then it would be able to detect any failures that were in the interconnecting electrical elements.
3) The harness is unlikely to be understood at the concept stage other than that the signal interface requirements will have to be met and so would be difficult to analyse.

The final implementation of the harness / interconnections / splices would be fully included when random hardware failures were evaluated to ensure that the safety goals were not violated as detailed in BS ISO 26262 part 3 clause 9 (BSI, 2011e), i.e. the connections have a greater impact on the reliability calculations than on the architectural metrics.

For analysis purposes the power supply can be considered as a part of the microcontroller in this approach. If the power supply fails, then it will affect the microcontroller which affects all elements classed as ‘Parameters’. If the power supply also powers sensors or actuators and the supply is critical in terms of accuracy of physical measurements or positional response of actuators, then it

may be necessary to add a measurement of voltage on the power supply so that any errors can be detected by a PCc. If the power supply was complex, which may be applicable in some automotive applications, then this approach would treat it as a system in its own right.

If we look at the control system in more detail, it is likely to contain a microcontroller to allow more complex control functions to be developed in software; this leads us to consider how this might be managed internally in terms of software variables. Generally, these are parameters used by subroutines that perform the control function. This allows the PCc to be thought of in terms of software variables but in reality, the analysis is performed on the hardware that manipulates or stores the variables.

Vehicles contain distributed systems interconnected by a communications system. For automotive control systems this is typically a Controller Area Network (CAN) bus (ISO, 2003), FlexRay bus (ISO, 2013) or Ethernet bus based on BroadR-Reach (Broadcom, 2014). Industrial systems use similar communications systems; some based on a CAN bus and others on Ethernet for example. Messages flow between the distributed nodes to communicate data signals from one area of the vehicle to another. These data signals can provide erroneous data so need to be considered when designing the conceptual architecture.

Actuators are another source of failures and must be considered, along with their associated output action from the control system.

3.5.2 Element Classification

To derive the classifications discussed below there were many of iterations before arriving at the final element proposal. This related to:

1) Data and Parameters. The conclusion was to keep these separate as the data is a specific interface and can be used between systems e.g. CAN bus, Local Interconnect Network (LIN) bus or within a system for example SPI, I^2C etc. but parameters are always within the internal memory area of the microcontroller or, if required, external memory e.g. calibration / configuration data.
2) Transducers / Measurement. Due to the simplicity of the measurement and complexity of the transducer, the result was to keep these as separate elements as it aids the analysis when reviewing the system description.
3) Power Supply Unit. The PSU is a common block, but it can be used in multiple places. The outcome was not to classify this as an element but still have a worksheet for an individual power supply. This can be applied to a relatively complex power supply i.e. one that supplies

the rails to a microcontroller. This is now shown as a PCc on the controller rather than an individual element and the diagnostic claim is then used as a line item in the SPFM and LFM architectural metrics calculation. The PCc can also be used in parameters where there is protection built in for the memory failures relating to power supplies. In the case of transducers, outputs and actuators the power supply can be included if safety critical and considered as an integral part of the element. It was decided that having the PSU as a separate item would clutter the system diagrams if included for each actuator, output, microcontroller, individual supply rail and impede system analysis.

In summary, when the architecture is analysed at the signal level, the system description must consider:

- **C**onnections.
- **M**easurements of voltage.
- **T**ransducers – conversion of physical measurements to a voltage prior to measurement i.e. Output (measured in Volts) = f(input)
- **D**ata - signals that pass between distributed systems or internally in control functions.
- **P**arameters – software variable used as inputs to control algorithms.
- **O**utputs – the output from a controller.
- **A**ctuators – control of physical outputs.

The above allows for any system to be analysed as all elements fit within the classifications. The first letters of the above list have been capitalised and can now be used to describe our simple control system in a way that is more suitable for analysis (Figure 6).

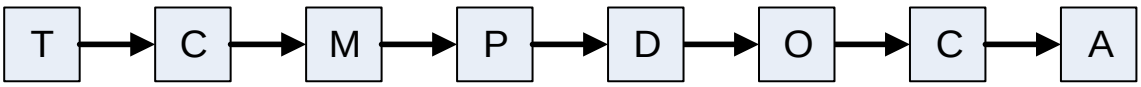


Figure 6: Simple system using abbreviations

The use of abbreviations has improved the way in which the system is viewed when identifying which types of faults occur at each categorised point. To be useful for analysis, further information is required to define the preliminary architecture:

- Signal name.
- Types of measurement.
- The sub system performing the control function.

The method for allocating components to specific items in the preliminary architecture is shown in Figure 7 (connections are not shown for clarity).

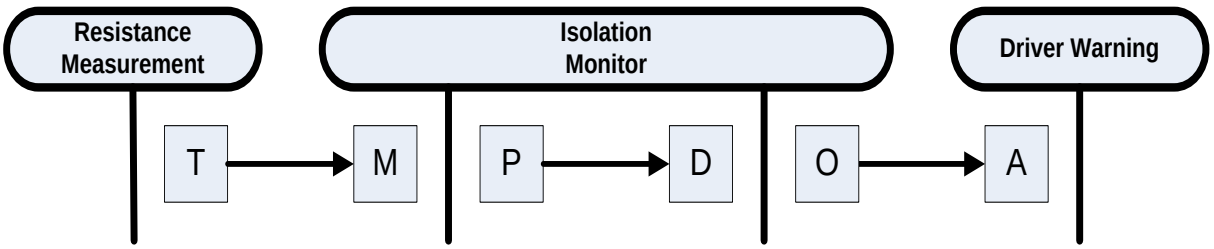


Figure 7: Simple system with preliminary architecture

The main aim of the work is to define the most appropriate architecture to achieve the required functional safety architectural metrics. When system architectures are analysed, it is useful to be able to differentiate between those elements that impact on functional safety and those that have no impact i.e. safe failures. For example, a power supply voltage may be measured and used for monitoring purposes. Any failure relating to this measurement may not violate the safety goal of interest for the item in terms of a single failure, but as it is used for diagnostics, it can still be considered as part a multiple point failure. The chosen route is to highlight any elements of interest in the functional safety analysis (Figure 8) in red and those that have no impact on functional safety in green. As the method evolved and additional diagnostic identification was included; if a signal is used purely for diagnostics or impacts on maintaining the safe sate it is shown in yellow.

In this case, the isolation resistance (ISOL_RES_AI_0V1, ISOL_RES_AI_AP_1kR and ISOL_WARN_DP) are all critical. The names may be considered slightly long but are unambiguous and unique within the design. The ISOL_RES_AP_1kR is purely used for diagnostics on the CAN Bus or it can be used as a self-test by monitoring by another system (connected to the CAN Bus). In this example, to demonstrate a safe signal, a power supply monitor is included purely for end of line test. The power supply has no impact on the safety goal and is not required for the diagnostics in relation to the isolation resistance measurement. As an interim solution where an element has not been classified then, as the concept is being developed, it initially remains black as previously shown in Figure 7.

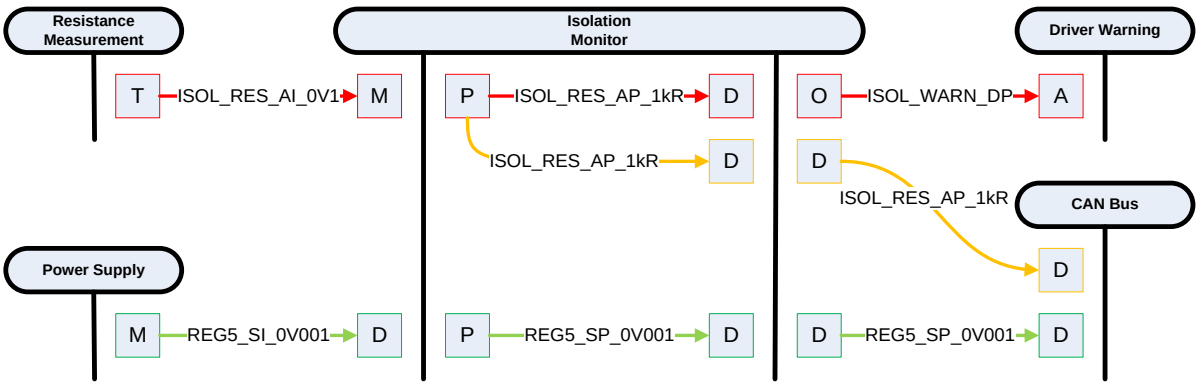


Figure 8: Simple system with safety impact shown

The vertical black lines indicate interfaces. This may be to the outside world as shown by the 'Resistance Measurement' or 'Driver Warning' for example or internal within the 'Isolation Monitor' where there is in interface to inputs and outputs with any internal processing shown within the two vertical lines.

3.5.3 Coverage Verification

In any safety critical design, it is important to continually verify that the design is correct and complete at the current point in time. This can equally be applied to process, which can be monitored by a checklist, as it can to component selection.

Considering detailed architectural metrics (part of the design process that must be completed to satisfy the safety critical design guidelines) against the conceptual design, the proposed method can be verified as shown in the following checklist (Table 10).

Table 10: Element Verification

Generic Hardware Description	Connectors	Measurements of voltage	Transducers	Data	Parameters	Outputs	Actuators	Verified
Electrical Elements	✓							✓
Processing Units					✓			✓
Non-volatile Memory					✓			✓
Volatile Memory					✓			✓
Analogue and Digital Inputs and Outputs		✓	✓			✓		✓
Communications Bus				✓				✓

Generic Hardware Description	Connectors	Measurements of voltage	Transducers	Data	Parameters	Outputs	Actuators	Verified
Power Supply					✓			✓
Program Sequence Monitoring / clock					✓			✓
Sensors			✓					✓
Actuators							✓	✓
Combinatorial and Sequential Logic					✓			✓

The element verification check does not cover systems. In this approach, the object that is being analysed is a system in itself. If the object is sufficiently complex that it can be considered a system in its own right, then this approach should be applied to it either:

1) As a separate exercise (assuming the object is in the design stage are of the lifecycle) with a defined interface to this system
2) Or as a combination of systems if it can't be broken down into independent systems, i.e. all the systems need to be included when considering violation of a safety goal.

If a system has already been designed, meets the relevant safety requirements for use in this application and it is being applied as intended, it can generally be treated as either a transducer i.e. it provides this higher-level system with a signal or as data i.e. it provides this system with a signal communicated over CAN bus for example or an actuator.

3.5.4 System Requirements

As more examples were completed the importance of a consistent naming convention became apparent. Significant improvements in traceability from initial concept through to final design can be realised if a naming convention for the Company is defined early on and used throughout the project and on subsequent projects.

3.5.4.1 Signal Naming Convention

The next stage is to understand the signals that transfer data between interfaces. This is achieved by labelling each signal in turn. In later stages of the design, i.e. when the hardware software interface is defined a naming convention would be applied, it is logical to apply the same convention to the signal name at the concept stage. This significantly aids traceability from the concept to final design and forces clear definition of signals very early on.

This structure can easily be adapted to suit a particular company. For this work, a generic structure and description shown in Table 11 has been developed. This can easily be expanded and tailored to suit an individual company process. To remove ambiguity, the naming convention must be consistent across all disciplines; systems, hardware, software and harness design engineers.

Table 11: Signal naming convention

Name	**Type**	**Direction**	**Units & Resolution**
Signal description e.g. **CELL1**	**_A** – Analogue **_Afb** – Analogue Feedback **_D** – Digital **_DH** – Digital high Side **_DL** – Digital Low Side **_F** – Frequency **_P** – PWM **_S** – Supply	**I'n'** - Input **O'n'** – Output **P** – Parameter **'n '** – Internal	**Units** **_A** – Current **_C** – Temperature **_Dg** – Degrees (angular) **_HI** – High **_Hz** – Frequency **_LO** – Low **_Pa** - pascal **_PC** - Per cent **_R** – resistance **_RX** – Receive (Note _RX max be prefixed by units and resolution for signals if required e.g. _0V1_RX) **_TX** – Transmit (Note _TX max be prefixed by units and resolution for signals if required e.g. _1C0_TX) **_V** – Volts **Resolution (where 'x' is replaced by 'Units')** **_0x000001** – x0.000001 resolution **_0x001** – x 0.001 resolution **_0x01** – x 0.01 resolution **_0x1** – x 0.1 resolution **_1x** – x 1 resolution **_kx** – x 1000 resolution **_Mx** x 1000000 resolution

Applying the convention for the resistance measurement signal is shown in Table 12:

Table 12: Isolation Resistance Signal Name

Name	**Type**	**Direction**	**Units**
ISOL_RES	_A	I	_1kR
abbreviated for 'Isolation Resistance'	it is analogue	and an input	and is measured in kΩ with a resolution of 1kΩ

In the system description diagram, this can be shown as 'ISOL_RES_AI_1KR'. When the signal is internal within an item the '_AI' may be removed as it is processed, but the rest of the name remains the same unless the resolution is changed by a function in which case the signal name would reflect this. All other signal names have been allocated in a similar fashion to generate the system description diagram shown in Figure 9. A specific example of an analogue signal (typically an input) is the _Afb signal which indicates internal analogue feedback. This may, for example, be a current measurement or voltage measurement provided by an intelligent high side output driver. To indicate resolution and scaling at this point in the design may seem pedantic, however if the software engineer requires a measurement accuracy of microvolts to perform a particular calculation and provide the necessary accuracy required in the final result, the hardware engineer will need to consider choice of analogue / digital converter in terms of resolution, range and noise floor. Bringing this level of understanding to signals (not necessarily components) at the concept stage introduces critical design decisions very early on and is beneficial when aiming for a right-first-time design. Resolution can be significant in the analysis of a PCc. An example would be in the case of a cell voltage measurement in a battery management system. These typically require an accuracy of 5mV, or better, to satisfy performance requirements. To achieve a PCc at this level would also require a sophisticated analogue front end and so may drive the choice of hardware.

The resistance measurement is shown as a transducer even though it measures the value as a voltage this is because in the final design it is likely that this will require some attenuation and scaling and so it is not a 'simple' voltage measurement.

In many cases, signals may pass through several components and need a different net list name on the schematic. The internal **'n'** term is used so for example the ISOL_RES_AI_1kR name would be used at the input, it this passed through a filter it would become ISOL_RES_AI1_1kR if this was necessary in order to support the final schematic layout tool.

Parameters (‘P’) are internal variables and so may not have a resolution or units, for example status flags or enumerated types.

If a resolution is not given, it is considered as non-critical. For example, a digital output may have a voltage output from a microcontroller to a high side driver which switches a load. These signals will have a required operating range (i.e. 12V, 24V) but the ‘_V’ is considered sufficient for the analysis work as the resolution will not affect performance or safety criticality. In the case of these signals it is useful to understand how the signal switches for the ‘ON’ state. For example, the ‘_D’ would use the designator ‘_DH’ to indicate a high side output (switches high to turn the output on) or ‘_DL’ if a low side output were used (switches low to turn the output on).

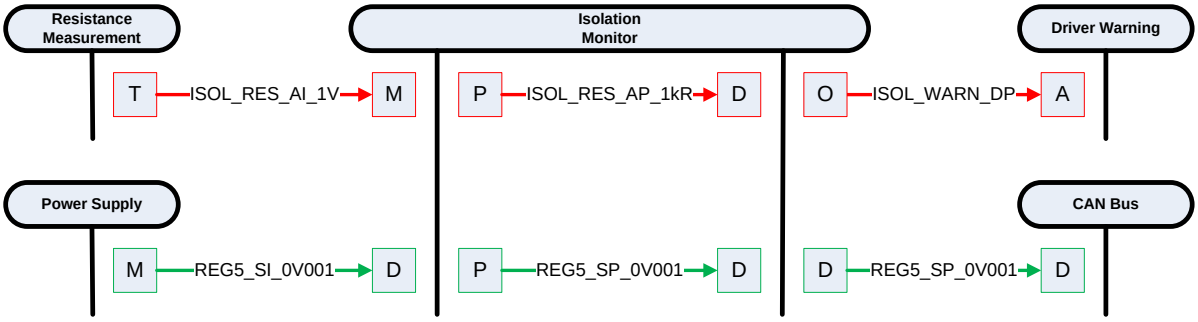


Figure 9: Simple system with safety impact and signal naming

3.6 Fault Consideration

The aim of the fault consideration section of the method is to ensure that all possible faults that may violate the safety goal of interest are known.

It is possible to consider what faults can occur at each element. BS ISO 26262 part 5 (BSI, 2011e) gives a table in Annex D of all faults that should be considered and their failure modes. For reference this has been included in Appendix C - Diagnostic Coverage Techniques as it references the analysis required to make claims for diagnostic coverage. The table is quite generalised and does not necessarily result in a full analysis of all failure modes, to achieve this a failure mode and effect analysis (FMEA) is recommended in BS ISO 26262 part 3 (BSI, 2011c). As the PCc method is aimed at the concept stage, the detail of the design is not yet known which makes a detailed, component level FMEA difficult. An FMEA (BSI, 2016) can theoretically be undertaken at any stage from a high-level block diagram down to the function of individual components. Based on this, an FMEA can be conducted at the concept stage, but this has limitations as it is a bottom up approach and so may need a greater level of detail than available at the concept stage. It is important not to add superfluous detail just to enable an FMEA to be completed at the concept stage. An FMEA useful

when examining signals in the system (once developed from the concept) and can identify significantly more specific signal-based failures than these already identified in BS ISO 26262 part 5 (BSI, 2011e) as these tend to be generic. To ensure that the PCc method has a high confidence level of covering all failure modes a number of techniques can be used. Some of these are discussed in BS ISO 26262 part 4 (BSI, 2011d) as methods for developing test cases for verification purposes. By bringing these methods into the concept stage it improves the identification of failure modes.

The methods discussed (BSI, 2011d) are:

- Analysis of external interfaces
- Analysis of internal interfaces
- Analysis of boundary values
- Error guessing based on knowledge or experience
- Analysis of functional dependencies
- Analysis of common limit conditions
- Analysis of sequences
- Analysis of sources of dependent failures
- Analysis of field experience

With all the faults determined for signals (the chosen method of analysis at the concept stage) through a combination of the above techniques the way in which they may affect the element classification can be tabulated. This leads onto the type of diagnostic coverage that is required to achieve the required percentage of diagnostic coverage. The robustness of the diagnostic coverage can be used in later analysis to understand the architectural metrics that are achieved by the design. By considering this early in the design the proposed method gives an accurate estimate of the architectural metrics that can be achieved by each preliminary architecture considered.

Failures will propagate from one element to another so the PCc can be used to show at which point in the system the failure is detected to prevent it propagating through the system to the output. If the failure is in the output element itself then the PCc will be some form of monitoring at the output.

An initial review of these requirements against the PCc method of classifying the elements (3.5.2) gives the following type of faults and failure mode allocation (Table 13).

Table 13: Fault Analysis and Failure Mode Consideration

	Element Classification						
	Connectors	**M**easurements	**T**ransducers	**D**ata	**P**arameters	**O**utputs	**A**ctuators
Open circuit	✓					✓	
High contact resistance	✓					✓	
Intermittent Contact	✓					✓	
Short circuit to ground (d.c. coupled)	✓					✓	
Short circuit to Vbat	✓					✓	
Short circuit / welded contact – always on						✓	
Short circuit – always off						✓	
Short circuit to neighbouring pin(s)	✓					✓	
Resistive drift between pins / signal lines	✓	✓					
Out of range		✓	✓	✓			
Offset		✓	✓	✓			
Stuck-in range		✓	✓	✓			
Drift		✓	✓	✓			
Oscillation		✓	✓	✓			
Power supply under and over voltage			✓		✓	✓	
Power supply drift and oscillation			✓		✓	✓	
Power spikes			✓		✓	✓	
Clock frequencies					✓		
Non-volatile Memory					✓		
Volatile memory / stack					✓		
ALU data path					✓		
Soft error model (single event transients)					✓		
Failure of communications				✓			
Message corruption				✓			
Message delay				✓			
Message loss				✓			
Unintended message				✓			

	Element Classification						
	Connectors	**M**easurements	**T**ransducers	**D**ata	**P**arameters	**O**utputs	**A**ctuators
Resequencing				✓			
Message insertion				✓			
Masquerading				✓			
Timeout / Arbitration / corruption / repetition				✓			
Incorrect action							✓
Delayed Action							✓

3.6.1 Safety Mechanism

Recognising the types of failure modes (Table 13) and having a conceptual understanding of the system function (for example, Figure 9), allows analysis of each of the elements in the system in order to determine safety mechanisms to detect and prevent all of the possible signal failures that can possibly result in a hazardous situation. The safety mechanism is the overall protection method covering detection of the fault (diagnostics), putting the system into a safe state and maintaining the safe state. This should occur in a maximum period of time referred to as the 'fault tolerant time interval' BS ISO 26262 part 1 (BSI, 2011a). This includes the diagnostic test interval (the time between diagnostic tests i.e. maximum time from a fault occurring to when it is detected by the safety mechanism), the fault reaction time (the time from detecting the fault to the system reaching a safe state) and the time that the system is in a safe state before a possible hazard can occur. The timing does not influence the architectural metrics but understanding the fault tolerant time interval when analysing the architectures may influence decisions on how diagnostics are implemented.

3.6.2 Diagnostic Coverage

To prevent faults influencing the operation of the system a method must be employed to detect all relevant failure modes that can violate a safety goal. These are generally termed diagnostic techniques and it is possible to assign a coverage percentage to the technique depending on its robustness and ability to diagnose the failure mode of interest.

The standards, for example BS ISO 26262 part 5 (BSI, 2011e) refer to specific diagnostic techniques that can be used to detect failures (as detailed in Appendix C - Diagnostic Coverage Techniques). The standard gives guidance on the maximum claim for different techniques. These tend to be very specific and are ideally suited to the later design stages where the final implementation is being

developed. However, a broader approach is required at the concept stage. The diagnostic coverage percentage claimed is critical to the SPFM, LFM and SFF calculations so it is important that the estimation is realistic at the concept stage for a new design. The estimate will increase in accuracy as the process is applied multiple times and final designs completed and analysed allowing re-use of techniques with fully verified diagnostic capability.

3.6.3 Plausibility Cross-check (PCc)

Strictly applying the diagnostic techniques implies that the system implementation is clearly understood but at this early stage in the design, these decisions have not yet been made. The PCc allows a more generic approach to be applied to diagnostics utilising standard diagnostic techniques as a reference point.

Plausible is defined as 'seemingly or apparently valid, likely, or acceptable; credible', which fits in with the aim of the method. This has been designated as a 'Plausibility Cross-Check' (PCc) as plausibility is demonstrated as a cross-check between two signals. This allows a more generalised method to be employed during the analysis which has a wider scope than a specific diagnostic coverage technique. Being generalised, the PCc may rely on several different diagnostic techniques in the concept stage.

For example, a PCc may be a simple valid range check. At the concept stage there may not be sufficient knowledge to know exactly how this algorithm will be implemented but it is acceptable to know that sufficient diagnostic coverage will be provided in the final design to ensure that the signal is in range (Figure 10) i.e. within a reference window. This takes a measured value and compares it with a calibration parameter to ensure the signal is within a window and outputs a failure signal when the signal is out of range.

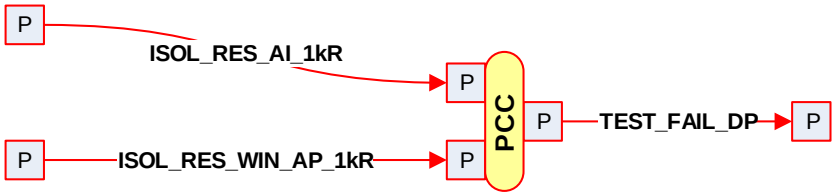


Figure 10: PCc example. Reference window for in-range monitoring

As the system design matures, the detail of the PCc is refined to the point where standard diagnostic coverage methods are employed for specific elements or components in the final design.

'Seemingly or apparently valid' is a qualitative term and insufficient for performing tangible engineering comparative analysis. The PCc must be quantified to allow a meaningful comparison to

be made between candidate architectures proposed at the concept stage in order to select an architecture to take forward with the confidence that the final design will be 'right first time'.

The PCc may not only be a comparison between two physical signals. It may be a comparison against a time reference for a rate of change measurement or measuring the delay between the activation of an output and an input signal affected by the output.

3.7 System Analysis

The method needs to have:

1) Traceable links to analysis methods used in the analysis of the final design.
2) Opportunity for continuous improvement so that as designs are completed any additional data acquired can be used to refine the PCcs for future designs.

3.7.1 Plausibility Cross-check Measures

For the PCc quantification to contribute to the design process it must provide a high confidence level that the final design will achieve the architectural metric targets that were predicted by the PCc analysis at the concept stage.

To achieve this, the method employed to evaluate architectural metrics in the final design must be clearly understood.

Generally, standards such as BS ISO 26262 part 5 (BSI, 2011e) and BS EN 61508 part 2 (BSI, 2010) use tables to map safety mechanisms and measures to achievable diagnostic coverage rankings. The rankings are rated low, medium and high and have respective diagnostic coverage levels of 60%, 90% and 99%. These percentages allow the PCc to be quantified by assigning a level to each PCc and then analysing the achievable Single Point Fault Metric (SPFM) and Latent-Fault Metric (LFM) in the case of BS ISO 26262 part 5 (BSI, 2011e) and Safe Fail Fraction (SFF) in the case of BS EN 61508 part 2 (BSI, 2010).

The SPFM and LFM can be calculated in a spread sheet based on the equations discussed in the following two sections.

3.7.1.1 Single Point Fault Metric (SPFM)

BS ISO 26262 part 5 (BSI, 2011e) defines the SPFM as the robustness of the item to single point and residual faults either by coverage from safety mechanisms or by design (primarily safe faults).

If the fault is a safe fault, when the fault occurs it does not lead to any increase in probability that the safety goal under consideration will be violated. It is important to remember that a component

may be considered safe when assessing one safety goal but considered a single point fault or residual fault when considering another safety goal. For example, an output failing open may be considered safe if the off state forces a warning lamp to come on and alert the driver.

In order to understand which components lead to a fault an FTA is typically used. Initially in the concept stage his may be qualitative and identify areas of the system that could violate the safety goal. As the design progresses and individual hardware components are identified then a full quantitative FTA can be populated to determine the probability of violation of the safety goal due to random hardware failures.

BS ISO 26262 part 1 (BSI, 2011a) has a number of specific definitions as detailed below:

A single point fault occurs when a fault without any safety mechanism occurs and leads directly to the violation of the safety goal under consideration.

A residual fault is a fault that is covered by a safety mechanism, but the safety mechanism is insufficient to prevent the fault from increasing the probability that the safety goal under consideration will be violated.

A multi-point fault is an individual fault that, in combination with other independent faults, leads to a multi-point failure. A multi-point failure is a failure resulting from the combination of several independent faults which leads directly to the violation of the safety goal.

The failure rate (λ), of each safety related hardware element according to BS ISO 26262 part 5 (BSI, 2011e) can be expressed according to Equation (1)

$$\boldsymbol{\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_{S}} \quad \textbf{(1)}$$

Where

$$\boldsymbol{\lambda_{SPF}}\ is\ the\ failure\ rate\ associated\ with\ the\ single\ point\ faults$$

$$\boldsymbol{\lambda_{RF}}\ is\ the\ failure\ rate\ associated\ with\ the\ residual\ faults$$

$$\boldsymbol{\lambda_{MPF}}\ is\ the\ failure\ rate\ associated\ with\ the\ multiple\ point\ faults$$

$$\boldsymbol{\lambda_{S}}\ is\ the\ failure\ rate\ associated\ with\ the\ safe\ faults$$

The single point fault metric can then be defined as (2)

$$\boldsymbol{SPFM = 1 - \frac{\sum_{SR,HW}(\lambda_{SPF} + \lambda_{RF})}{\sum_{SR,HW}\lambda} = \frac{\sum_{SR,HW}(\lambda_{MPF} + \lambda_{S})}{\sum_{SR,HW}\lambda}}$$

(2)

Substituting (1) into (2) this can be rewritten as (3)

$$\boldsymbol{SPFM == \frac{\sum \lambda_S + \sum \lambda_{MPF}}{\sum \lambda_{SPF} + \sum \lambda_{RF} + \sum \lambda_{MPF} + \sum \lambda_s}}$$

(3)

3.7.1.2 Safe Fail Fraction (SFF)

BS EN61508 part 2 (BSI, 2010) defines the SFF as the property of a safety related element that is defined by the ratio of safe plus dangerous detected failures and safe plus dangerous undetected failures.

The failure rate (λ), of each safety related hardware element can be expressed (BSI, 2010) according to Equation (4).

$$\boldsymbol{\lambda = \lambda_S + \lambda_{Dd} + \lambda_{Du}}$$

(4)

Where

$\boldsymbol{\lambda_S}$ *is the failure rate associated with the safe faults*

$\boldsymbol{\lambda_{Dd}}$ *is the failure rate associated with the dangerous detected faults*

$\boldsymbol{\lambda_{Du}}$ *is the failure rate associated with the dangerous undetected faults*

The safe fail fraction is then defined as (5).

$$\boldsymbol{SFF = \frac{\sum \lambda_s + \sum \lambda_{Dd}}{\sum \lambda_s + \sum \lambda_{Dd} + \sum \lambda_{Du}}}$$

(5)

3.7.1.3 Comparing SPFM and SFF

On first inspection the equations for SFF (5) and SPFM (2) look rather different, however, by examining the descriptions for each of the failure rates it can be shown that they both calculate the same metric. Replacing λ_s with λ_{safe} to avoid confusion with λ_s in the SPFM equation gives (6).

$$\boldsymbol{SFF} = \frac{\sum \boldsymbol{\lambda_{safe}} + \sum \boldsymbol{\lambda_{Dd}}}{\sum \boldsymbol{\lambda_{safe}} + \sum \boldsymbol{\lambda_{Dd}} + \sum \boldsymbol{\lambda_{Du}}}$$

(6)

As the approach in BS EN61508 part 2 (BSI, 2010) does not consider multiple point faults they can be considered as not dangerous i.e. safe so can be derived.

$$\boldsymbol{\lambda_{safe}} = \boldsymbol{\lambda_s} + \boldsymbol{\lambda_{MPF}}$$

(7)

Substituting (7) into (6) gives

$$\boldsymbol{SFF} = \frac{\sum \boldsymbol{\lambda_s} + \boldsymbol{\lambda_{MPF}} + \sum \boldsymbol{\lambda_{Dd}}}{\sum \boldsymbol{\lambda_s} + \boldsymbol{\lambda_{MPF}} + \sum \boldsymbol{\lambda_{Dd}} + \sum \boldsymbol{\lambda_{Du}}}$$

(8)

In BS ISO 26262 part 5 (BSI, 2011e) all dangerous detected faults are considered safe so can be grouped as λ_s giving (9).

$$\boldsymbol{SFF} = \frac{\sum \boldsymbol{\lambda_s} + \boldsymbol{\lambda_{MPF}}}{\sum \boldsymbol{\lambda_s} + \boldsymbol{\lambda_{MPF}} + \sum \boldsymbol{\lambda_{Du}}}$$

(9)

BS ISO 26262 part 5 (BSI, 2011e) also considers dangerous undetected faults to be the sum of single point faults and residual faults (10). This allows the residual faults to be considered under an additional metric – latent fault metric (LFM)

$$\boldsymbol{\lambda_{Du}} = \boldsymbol{\lambda_{SPF}} + \boldsymbol{\lambda_{RF}}$$

(10)

Substituting (10) into (9) gives

$$SFF = \frac{\sum \boldsymbol{\lambda_s} + \sum \boldsymbol{\lambda_{MPF}}}{\sum \boldsymbol{\lambda_s} + \boldsymbol{\lambda_{MPF}} + \sum \lambda_{SPF} + \sum \lambda_{RF}}$$

(11)

Referring back to (3) proves that the single point fault metric and the safe fail fraction are actually identical (12).

$$\boldsymbol{SFF} = \boldsymbol{SPFM}$$

(12)

This is acceptable as far as single faults are concerned but in terms or architectural analysis BS ISO 26262 considers the Latent Fault Metric and BS EN 61508 considers hardware fault tolerance.

3.7.1.4 Latent Fault Metric

BS ISO 26262 part 5 (BSI, 2011e) also calls for latent faults to be analysed for high higher ASIL safety goals. A latent fault is described as multiple-point fault whose presence is not detected by a safety mechanism nor perceived by the driver within the multiple point fault detection interval BS ISO 26262 part 1 (BSI, 2011a). This covers all multi-point faults; however, the standard is quite clear that in the majority of cases the analysis only needs to be applied to dual point faults (not higher order unless considered necessary). It is important to analyse the technical safety concept to ensure that as a minimum, if one fault affected a safety related element that a second fault does not affect the corresponding safety mechanism. If this were to happen then it is possible that a fault occurs and then then system cannot achieve or maintain the safe state due to the second fault.

In redundant systems, additional rigour in the analysis may be required to look at triple point or higher order faults depending on the redundancy and safety mechanisms built into the safety concept.

When considering the safety mechanism, it is important to consider all attributes, including detection, entering a safe state, maintaining a safe state and the time intervals to achieve these attributes.

3.7.2 SPFM and LFM calculations

As the SPFM and LFM are calculated in a spreadsheet it is appropriate to use a similar approach in the PCc quantification. The spreadsheet (headings shown in Table 14) requires a significant amount of data to populate it and subsequently perform the SPFM and LFM calculations. It must be remembered that this calculation needs to be performed for each safety goal with a sufficiently high enough ASIL rating to require the calculations to be performed according to the applicable standard. Due to the improvement in diagnostics offered, the author would recommend performing PCc analysis at all safety integrity levels.

Table 14: Architectural Metrics Calculation Headings

Component Description	Failure Rate (FIT)	Safety Critical	Failure Mode	Failure Mode Distribution (%)	Safety Goal Violation	Safety Mechanism	Diagnostic Coverage (%)	Single Point (FIT)
Single Point Fault Metric								%

The data required for the final design calculation is discussed in sections 3.7.2.1 to 3.7.2.9.

3.7.2.1 Component Description

Allocated at the final design stage, this is at the electrical / electronic component level i.e. integrated circuit, microcontroller, capacitor, resistor, crystal etc.

3.7.2.2 Failure Rate (FIT)

The failure rate of the component. This is often available from the supplier of the device. If not, it is possible to use generic data. Isograph products such as reliability Workbench (Isograph, 2017) reference several typical databases such as MIL-HDBK-217, Telcordia SR-332, Quanterion 217 Plus, IEC TR 62380, NSWC, GJB/z 299B and 299C, and Siemens SN29500. Failures in time (FIT) is often used as it represents the number of failures that can be expected per one billion (10^9) device-hours of operation. This can be one failure in one device in 10^9 hours or operation of 1 failure in one thousand (10^3) devices operating for one million (10^6) hours etc.

3.7.2.3 Safety Criticality

Whether the component is considered safety critical or not. If any of the failure modes for the component can lead to the violation of the safety goal, as determined by FTA discussed earlier (3.7.1.1), then it should be considered safety critical and the quality of the component source, storage, usage etc. controlled accordingly.

3.7.2.4 Failure Mode

This details each of the failure modes of the component. These were derived in section 3.6. As this is for the final design calculation, the failure modes should be assessed (through independent review) to ensure that every possible failure mode has been identified. It is important that all failure modes are covered whether they are considered safe or non-safe. This improves analysis efficiency as a base spreadsheet can be generated and used for each safety goal in the knowledge that all failure modes for all components are validated.

3.7.2.5 Failure Mode Distribution (%)

Distribution of the failure mode can be found from component suppliers, generic handbooks or from analysis performed by the manufacturer on returned products (warranty or repair). An example is that a component with two failure modes 'A' and 'B' may fail in mode 'A' 80% of the time and mode 'B' 20% of the time. The failure modes can be as straightforward as short circuit and open circuit for example. If data cannot be obtained from the specific component manufacturer or from warranty data then a useful source is provided by the System Reliability Centre (System Reliability Centre, 2001). This is useful for both electronic and mechanical components; although mechanical components are outside the scope of BS ISO 26262, the data may be useful when considering external mechanical measures of risk reduction / failure mitigation at electronic / physical interfaces.

3.7.2.6 Safety Goal Violation

The SPFM and LFM calculations are performed for each safety goal so the engineer must be able to determine whether the failure mode for this component violates the safety goal or not. It is not uncommon for a system with two safety goals, '1' and '2' to have a component that fails in mode 'A' and violates safety goal 1 and fails in mode 'B' and violates safety goal 2. This can cause real design problems when selecting components for function and cost and having to meet conflicting safety goals and their associated ASIL rating.

3.7.2.7 Safety Mechanism

The failure mode of the component should, where necessary, be detected by some form of safety mechanism. It is important that this is traceable and verifiable in the design. It should be possible to identify the safety mechanism and ideally understand how it fits into the mechanisms discussed in the guidelines being applied and the maximum diagnostic coverage percentage (3.7.2.8) that can be allocated to the mechanism.

3.7.2.8 Diagnostic Coverage (%)

Generally rated as low (60%), medium (90%) and high (99%), the DC percentage quantifies what percentage of this failure mode will be detected by the safety mechanism (3.7.2.7).

3.7.2.9 Single Point (FIT)

The failure rate calculated for each failure mode that can violate the safety goal.

3.7.3 Analysis of Plausibility Cross-Checks

By understanding how the final design architecture is analysed (3.7.2) a method can be formulated to analyse the PCC at the concept stage to quantitatively compare candidate architectures.

Generally, at the concept stage, signals are identified as they are derived from inputs, migrate through the system and are used to generate outputs. There is no knowledge of the actual electronic component data as required in the SPFM and LFM calculations (3.7.2). This section discusses how the PCc is quantified to allow the architectural metrics to be calculated at the concept stage by looking at each piece of data required for the SPFM and LFM calculations again to see how the data can be obtained at the concept stage.

Two possible areas of concern detailed (Lundteigen & Rausand, 2006) are increasing the safe failures by inclusion on non-essential function failures and using different assumptions for calculation of the metrics.

This method avoids these pitfalls as far as possible by:

1) Limiting the calculation:
    a. To the specific safety goal under consideration (a requirement in BS ISO 26262)
    b. Minimising the architecture through element classification to those elements which are safety critical, i.e. functions non-essential to the safety goal (which would tend to have safe failures) are not included in the analysis.
2) Using the same assumptions for the elements in each of the candidate architectures. This avoids variance in for example the assumptions made by different vendors when performing the calculations, i.e. variance in failure rate data, failure mode distribution and diagnostic coverage percentages.

3.7.3.1 Failure Rate

As per the element classification (3.5.2) the conceptual analysis works at a much higher level. This means allocating a failure rate to elements (lumped models) used in the PCc analysis.

When the final design is not known, estimating the failure rate requires a certain level of engineering judgement. This can be broken down into three different maturity levels:

1) Completely new design with no previous PCc analysis performed (3.7.3.1.1).
2) New design where PCc analysis has been performed previously on different systems (3.7.3.1.2).
3) Design of a new controller based on previously analysed building blocks with known correlations between PCc predicted SPFM / LFM and that achieved in the final design (3.7.3.1.3).

As discussed in 2.11, care must be taken to ensure that the architectural metrics are not biased by significant differences in failure rate for different components. Taking the SPFM as an example with two components with an order of magnitude difference in failure rate but similar diagnostic coverage a high (90%) SPFM percentage is achieved (Table 15).

Table 15: SPFM Example - 90% DC on both Components

Failure Rate (FIT)	Safety Critical Failure Allocation (%)	Safety Critical Failure Rate (FIT)	Diagnostic Coverage (%)	Single Point or Residual Failure Rate (FIT)
10	50%	5	90%	0.5
1	50%	0.5	90%	0.05
			SPFM	90%

However, if we now allocate a low diagnostic coverage percentage on the component with the high failure rate a SPFM percentage of 17% is achieved (Table 16).

Table 16: SPFM Example - 10% DC on High Failure Rate Component

Failure Rate (FIT)	Safety Critical Failure Allocation (%)	Safety Critical Failure Rate (FIT)	Diagnostic Coverage (%)	Single Point or Residual Failure Rate (FIT)
10	50%	5	10%	4.5
1	50%	0.5	90%	0.05
			SPFM	17%

If the low diagnostic coverage is now applied to the low failure rate component the SPFM returns to 83% (Table 17).

Table 17: SPFM Example - 10% DC on Low Failure Rate Component

Failure Rate (FIT)	Safety Critical Failure Allocation (%)	Safety Critical Failure Rate (FIT)	Diagnostic Coverage (%)	Single Point or Residual Failure Rate (FIT)
10	50%	5	90%	0.5
1	50%	0.5	10%	0.45
			SPFM	83%

The above three examples show that consideration must be given to high failure rate components (or lumped models) when undertaking the architectural metric calculations. If necessary, similar component types can be grouped by order of magnitude of failure rate and the metrics calculated separately to determine the architectural metrics.

Generally, the concept failure rates are lumped models for elements (discussed in 3.7.3.1.1). Moving from the conceptual stage to the full analysis means that the difference is averaged out due to the higher number of components in the analysis.

3.7.3.1.1 Maturity Level 1

In this case, it is probable that the company has previously designed electronic control units and understands failure rates. This may be for simple reliability analysis for warranty purposes or more detailed analysis from a safety perspective. An estimation can be made for each of the classified elements (3.5.2) by taking a sum of failure rates for an estimated number of components in the classified block.

Taking a relatively trivial example, a voltage measurement input may logically consist of a potential divider, low pass filter and clamping diode. An estimate of the number of components, the type of components and a generic failure rate (Table 18) can be given as:

Table 18: Failure Rate Estimation

Component	Quantity	Failure Rate (FIT)	Total Failure Rate (FIT)
Resistor	2	0.224	0.448
Capacitor	2	0.08	0.16
Diode	1	0.71	0.71
		Element Failure Rate (FIT)	1.318

If this value for the failure rate is used in all candidate architectures, conclusions can be drawn as to which architectures offer improvements in achievable architectural metrics. As more information is accrued during the conceptual design, these values can be optimised and carried over into all architectures to give a better prediction for the architectural metrics.

3.7.3.1.2 Maturity Level 2

Where possible, previous analysis work will be used. For example, if a similar circuit was to be used for voltage measurement as above (3.7.3.1.1), the actual number of components and more representative failure rates are used in the final design or prototype designs would be used. This should be achievable, even to companies new to projects with additional safety critical design aspects.

3.7.3.1.3 Maturity Level 3

As more projects are completed it is possible to further refine the failure rate data. Maybe on earlier designs, problems were found with ESD protection on several inputs and so additional filtering and transient protection are added to the original voltage input circuits to be used for future designs. Rather than using generic failure rates as in Maturity Level 1 and 2, the actual failure rate for each individual component is now known and so a more accurate lumped value for the voltage input block can be used in the PCc analysis. Additional detail, may, for example, be that although two capacitors are used they have different dielectric materials and so different failure rates. Including this data provides a more accurate overall failure rate for the lumped model.

3.7.3.2 Safety Criticality

This has the same meaning in the PCc analysis except that it now relates to the 'element' under consideration in the PCc rather than the 'component' in the final design.

3.7.3.3 Failure Mode

The analysis has moved from single components to a lumped model (components combined to form an element). In Table 13, the failure modes for consideration were listed against each element classification. These can be defined and failure mode distribution percentages allocated to each failure mode that needs to be considered in the PCc for each element. These are examined individually for each classification in the following sections.

3.7.3.3.1 Connectors

The connector category covers harnesses splices and connectors. In automotive applications the harnesses can be a major cause of faults due to the harsh environmental conditions. This includes

temperature, humidity, corrosion, vibration etc. Good design practices mitigate many of these failures and only knowledge of the electrical harness, physical layout, mechanical restraints and historical data for similar applications can provide the actual failure mode distribution. However, an initial estimate can be taken from the view that the vehicle chassis is normally connected to the ground of the low voltage electrical power supply (commonly 12V for cars and 24V for commercial vehicles and now with mild hybrids 48V to reduce current ratings) so if wire insulation wears through then it is more likely to short to ground than any other voltage. Another frequent problem is wires breaking through long term fatigue or pins backing out of connectors. Continued analysis of the possible failures results in an initial estimate (based on experience) of failure mode distribution as indicated in Table 19.

Table 19: Failure Mode Distribution for Connectors

Element	**Analysed Failure modes for low / medium / high Diagnostic Coverage**			**Failure Mode Distribution**
	Low	**Medium**	**High**	
	60%	**90%**	**99%**	
Harness including splice and connectors	Open Circuit	Open Circuit	Open Circuit	**20%**
			Contact resistance	**10%**
	Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	**30%**
		Short Circuit to Vbat	Short Circuit to Vbat	**20%**
		Short circuit between neighbouring pins	Short circuit between neighbouring pins	**10%**
			Resistive drift between pins / signal lines	**10%**

3.7.3.3.2 Measurements

To a certain extent, the failure modes applicable to measurements are like those of connectors. The main additions being offsets, stuck in range and drift and oscillation. Again, distribution percentages (Table 20) are estimated based on current knowledge and refined as more historical data becomes available within the Company through warranty returns, diagnosed failures and reported diagnostic trouble codes (DTC's).

Table 20: Failure Mode Distribution for Measurements

Element	**Analysed Failure modes for low / medium / high Diagnostic Coverage**			**Failure Mode Distribution**
	Low	**Medium**	**High**	
	60%	**90%**	**99%**	
Harness including splice and connectors			Resistive drift between pins / signal lines	**15%**
Analogue and digital Inputs	Open circuit	Open circuit	Open circuit	**10%**
	Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	**15%**
		Short Circuit to Vbat	Short Circuit to Vbat	**10%**
		Short circuit between neighbouring pins	Short circuit between neighbouring pins	**10%**
		Offsets	Offsets	**15%**
	Stuck in range	Stuck in range	Stuck in range	**15%**
		Drift & Oscillation	Drift & Oscillation	**10%**

3.7.3.3.3 Transducers

As discussed previously, Transducers are considered more complex than Measurements and so are likely to either:

1) Have their own internal power supply
2) OR rely on a stabilised power supply from a dedicated sensor power supply or a sensor supply output from a main ECU.

For this reason, power supplies are considered as part of the Transducer analysis along with the normal Transducer failure modes (Table 21).

Table 21: Failure Mode Distribution for Transducers

Element	**Analysed Failure modes for low / medium / high Diagnostic Coverage**			**Failure Mode Distribution**
	Low	**Medium**	**High**	
	60%	**90%**	**99%**	
Sensors including Signal Switches	Out of range	Out of range	Out of range	**20%**
		Offsets	Offsets	**10%**
	Stuck in range	Stuck in range	Stuck in range	**30%**
			Oscillation	**5%**
Power supply	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	**10%**
		Drift	Drift & Oscillation	**20%**
			Power Spikes	**5%**

3.7.3.3.4 Data

For PCc analysis the failure modes relating to Data cover two areas; the sensors and the actual data transmission. This is more appropriate in automotive applications as there tend to be distributed systems and so one ECU may make a measurement or have a sensor connected to it. The ECU may then transmit this data over the CAN bus for further processing in another ECU. Estimates are given for failure mode distribution in Table 22.

Table 22: Failure Mode Distribution for Data

Element	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution
	Low	**Medium**	**High**	
	60%	**90%**	**99%**	
Sensors including Signal Switches	Out of range	Out of range	Out of range	**30%**
		Offsets	Offsets	**10%**
	Stuck in range	Stuck in range	Stuck in range	**30%**
			Oscillation	**4%**
Data Transmission	Failure of communication peer	Failure of communication peer	Failure of communication peer	**15%**
	Message corruption	Message corruption	Message corruption	**2%**
	Message Delay	Message Delay	Message Delay	**3%**
	Message Loss	Message Loss	Message Loss	**2%**
	Unintended message repetition	Unintended message repetition	Unintended message repetition	**1%**
		Resequencing	Resequencing	**1%**
		Insertion of message	Insertion of message	**1%**
			Masquerading	**1%**

3.7.3.3.5 Parameters

Parameters are the most complex classification to analyse due to them being microcontroller based i.e. they are processing data in a microcontroller, which, as well on relying on a power supply and external clock or oscillator they also have complex internal memory, processing units and peripheral blocks. Initial estimates are given in Table 23, however, data from manufacturers specifically on the microcontroller may provide a better distribution percentage if the silicon manufacture is willing to divulge this information. This type of data is difficult to analyse based on returns as most ECU design companies would only be able to narrow down failures to the complete microcontroller or specific peripheral pins. Internal diagnosis would not be possible but may be achievable by the manufacturer using built-in test code used for end-of-line test.

Table 23: Failure Mode Distribution for Parameters

Element	**Analysed Failure modes for low / medium / high Diagnostic Coverage**			**Failure Mode Distribution**
	Low	**Medium**	**High**	
	60%	**90%**	**99%**	
Power supply	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	**10%**
		Drift	Drift & Oscillation	**10%**
			Power Spikes	**5%**
Clock	stuck at	stuck at	stuck at	**5%**
		dc fault model	dc fault model	**5%**
			Incorrect frequency	**10%**
			Period jitter	**10%**
Non-volatile Memory	stuck at	stuck at	stuck at	**5%**
		dc fault model	dc fault model	**5%**
Volatile Memory	stuck at	stuck at	stuck at	**5%**
		dc fault model	dc fault model	**5%**
		soft error model	soft error model	**5%**

Element	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution
	Low	**Medium**	**High**	
	60%	**90%**	**99%**	
Processing Units: ALU - Data Path	Stuck at	Stuck at	Stuck at	**5%**
		Stuck at - gate level	Stuck at - gate level	**5%**
			dc fault model	**5%**
Processing Units: ALU - Data Path			Soft error model for sequential parts	**5%**

3.7.3.3.6 Outputs

Outputs consider both analogue and digital outputs. For PCc analysis it is assumed that the power supply is also critical in the case of both high side digital outputs and analogue outputs and so has been included in Table 24. This includes devices such as intelligent high side or low side switches.

Table 24: Failure Mode Distribution for Outputs

Element	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution
	Low	**Medium**	**High**	
	60%	**90%**	**99%**	
Analogue and digital Outputs - stuck at	Open circuit	Open circuit	Open circuit	**15%**
	Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	**15%**
		Short Circuit to Vbat	Short Circuit to Vbat	**10%**
		Short circuit between neighbouring pins	Short circuit between neighbouring pins	**10%**
		Offsets	Offsets	**5%**
	Stuck in range	Stuck in range	Stuck in range	**10%**
			Drift & Oscillation	**5%**
Power supply	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	**5%**
		Drift	Drift & Oscillation	**20%**
			Power Spikes	**5%**

3.7.3.3.7 Actuators

Actuators can be relatively straightforward, such as a warning lamp or be a complex system in their own right, for example an actuator in an Automated Manual Transmission (AMT). This is detailed as a final element in Table 25 and for a full analysis would require a similar amount of work to the main control system. However, when performing PCc analysis it is sufficient to consider just the three types of elements, output relays, power supply and final elements. Actuators normally also rely on power supplies and often in automotive systems relays or intelligent switches are used to switch high current loads.

Table 25: Failure Mode Distribution for Actuators

Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution
		Low	**Medium**	**High**	
		60%	**90%**	**99%**	
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	**20%**
		Welded Contacts	Welded Contacts	Welded Contacts	**5%**
			Individual welded contacts	Individual welded contacts	**10%**
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	**10%**
			Drift	Drift & Oscillation	**15%**
				Power Spikes	**5%**
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	**10%**
				Incorrect action	**15%**
				Delayed Action	**10%**

3.7.3.3.8 Power Supplies

Power supplies can be relatively complex systems and may need to be considered separately (Table 26) and for a full analysis may require a similar amount of work to the main control system.

Table 26: Failure Mode Distribution for Power Supplies

Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution
		Low	**Medium**	**High**	
		60%	**90%**	**99%**	
Power Supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	**50%**
			Drift	Drift & Oscillation	**20%**
				Power Spikes	**30%**

3.7.3.4 Failure Mode Distribution

The failure mode distribution is now based on the element failure modes and as discussed above, additional failure modes may need to be considered when looking at a single element in the final design SPFM and LFM.

A level of experience exists on the accuracy of failure mode distribution as it did in the failure rate section (3.7.3.1) and this accuracy will improve as more designs are completed using safety critical design techniques and processes, i.e. as the design progresses and analysis of in-field failures mature.

3.7.3.4.1 Maturity Level 1

An estimation can be made for each of the classified elements (3.5.2) by using standard databases as discussed in 3.7.2.2. Another useful source is internal company information where data has been recorded over many years.

If the final component arrangement or perhaps even the polarity of the signal were unknown i.e. failing high can be safe and failing low can be dangerous or vice-versa then a failure mode distribution of 50% can be assumed. If these values for failure rate and failure mode distribution were used in all candidate architectures, then conclusions can be drawn as to which architectures offer improvements relative to each other in achievable safety integrity level. However, the 50%

assumption will impact on the absolute error in the PCc SPFM and LFM results. As more information is accrued during the conceptual design, these values should be optimised and again carried over into all architectures to give a better prediction for the architectural metrics.

3.7.3.4.2 Maturity Level 2

Where possible, previous analysis work will be used. For example, if a similar circuit for voltage measurement as above (3.7.3.1.1) is used; it may be that the only dangerous failure occurs when the sensor input fails high or in range. The failure mode estimation for this may be a total of 10% for example and so the dangerous failure mode is now only attributed to 10% of the failure rate not 50% as in maturity level 1. If this new failure mode percentage is propagated through all candidate architectures, then accuracy of the achievable safety integrity level is improved.

3.7.3.4.3 Maturity Level 3

As more projects are completed it is possible to refine the failure mode distribution. As actual failure modes are obtained through testing and early prototype data is further refined.

3.7.3.5 Safety Goal Violation

In the PCc method the safety goal can be violated by an element rather than the component. This decision based on element failure modes is simplified compared to the component level failure modes where detailed electrical circuit analysis may be required to understand whether the safety goal is violated or not.

3.7.3.6 Safety Mechanism

The safety mechanism is now made up of several different diagnostic techniques. It is important that each technique is defined and understood as these techniques will carry over and be employed in the final design. This is considered an advantage at this stage because the concept is already formulating requirements for the final design and can be a useful validation check against the hardware software interface specification that will be defined in the system design stage of the project BS ISO 26262 part 4 (BSI, 2011d).

3.7.3.7 Diagnostic Coverage

Diagnostic coverage now details the diagnostic coverage achieved by the PCc. To define this, all of the diagnostic techniques applicable to an element are grouped. This allows each technique to be allocated a diagnostic coverage percentage and these combined to calculate the achievable diagnostic coverage for the PCc for the element. This approach has major benefits:

1) It is rigorous in the method used to analyses each DC percentage.

2) It achieves the same level of detailed analysis as will be performed on the detailed design but is much faster as it considers lumped elements and signals rather than individual components.
3) The tables used contain the detail of each PCc, the associated diagnostic techniques and the expected diagnostic coverage which allows a direct comparison to be made not only in relation to requirements validation but also in terms of achieved metrics.

3.7.4 Plausibility Cross-Check Quantification

The PCcs are designed to align with the techniques described in BS ISO 26262 part 5 (BSI, 2011e). There are a few reasons for adhering to this policy:

1) The techniques are well known across a number of standards and have roots in BS EN 61508 part 2 Annex A (BSI, 2010), meaning that the techniques can be used in all control applications, such as, machinery, industrial and automotive.
2) Close alignment to the standard at the conceptual stage leads to close alignment at the analysis stage which provides a more robust explanation, or more explicitly, an argument as discussed by Kelly (Kelly, 2003) when developing the safety case for example using Goal Structured Notation (GSN).
3) The techniques are proven, well documented and have justified maximum diagnostic claims depending on the robustness of the technique applied.

3.7.4.1 PCc Claim Calculation

The PCc claim is calculated based on the factors described in this section. To simplify application of the method the calculation has been converted to a macro which can be run in a spreadsheet (3.7.4.3). The calculation is interpreted from the ISO 26262 part 3 (BSI, 2011e). The calculation will be the same for both the concept design using the PCc and the final design which looks at the diagnostic coverage for each individual component.

Initially the Failure Mode Diagnostic Coverage (***FMDC***) is calculated (13). This depends on whether:

1) The failure mode for the lumped model can violate the safety goal (***FMvSG***), this is set to 1 if the failure mode for the lumped model will violate the safety goal under consideration, otherwise it is 0.
2) An Available Technique is Used (***ATU***), this is set to 1 if a technique is used, otherwise it is 0. Generally, techniques are taken from ISO26262 part 5 (BSI, 2011e), but with justification other techniques could be used.

3) The Maximum Claim for the Technique used (***MCfT***). This is set to 60% for low, 90% for medium and 99% for high diagnostic coverage, assuming available techniques from ISO 26262 part 5 (BSI, 2011e) are used and implemented to their full capability. These percentages will require justification in the final implementation.

$$\boldsymbol{FMDC = (FMvSG\ x\ ATU\ x\ MCfT)} \quad \textbf{(13)}$$

Where

$$\boldsymbol{FMvSG} - Failure\ Mode\ Violates\ Safety\ Goal$$

$$\boldsymbol{ATU} - Available\ Technique\ Used$$

$$\boldsymbol{MCfT} - Maximum\ Claim\ for\ Technique$$

It is only possible to make a claim for a minimum diagnostic coverage if all the failure modes have an associated technique utilised in the design to detect the failure mode. For example, if, in order to achieve low (60%) diagnostic coverage for an element it must be possible to detect open circuit and short circuit to ground and both failure modes have diagnostic coverage then up to 60% can be claimed. However, if one of the failure modes is not covered then this claim cannot be made. The Maximum Claim for Failure Mode Diagnostic Coverage (MCFMDC) is limited (14) based on whether all failure modes are covered for each of the low, medium and high diagnostic coverage claims.

$$\boldsymbol{MCFMDC = f(FMDC, AFMDl, AFMDm, AFMDh)} \quad \textbf{(14)}$$

Where

$$\boldsymbol{AFMDl} - All\ Failure\ Modes\ Detected - low$$

$$\boldsymbol{AFMDm} - All\ Failure\ Modes\ Detected - medium$$

$$\boldsymbol{AFMDh} - All\ Failure\ Modes\ Detected - high$$

This function will limit the **MCFMDC** to 0%, 60%, 90% or 99% accordingly.

For the failure mode of an element that violates the safety goal, the failure mode distribution factor must be known. For example, if the failure mode under consideration is open circuit and this contributes 20% of the overall failure rate then the Element Failure Mode Contribution (**EFMC**) would be set to 20%.

The Failure Mode Diagnostic Coverage Claim (**FMDCC**) can now be calculated (15).

$$\boldsymbol{FMDCC = (MCFMDC\ x\ EFMC\ )} \quad \textbf{(15)}$$

Where

$$\boldsymbol{MCFMDC} - Maximum\ Claim\ for\ Failure\ Mode\ Diagnostic\ Coverage$$

$$\boldsymbol{EFMC} - Element\ Failure\ Mode\ Contribution$$

3.7.4.2 PCc Confidence Levels

The PCc confidence level was developed for many reasons:

a) It allows for a certain amount of flexibility at the concept stage. Various techniques can be used to diagnose a specific failure mode and the final technique may not be known so more than one technique can be referenced in the concept. As the design develops at least one of these techniques must be carried forward and the techniques employed in the final design must have comparable diagnostic coverage claims. If the technique(s) chosen cannot achieve the level claimed then additional techniques as used in the PCc can be deployed to increase diagnostic coverage.

b) As the design develops then a limited number of techniques may be used in the final implementation but the chosen techniques will be fully developed to the point where it approaches or meets full diagnostic coverage claim and is therefore justified. This means that a conservative PCc DC% claim may achieve a higher diagnostic coverage percentage in the final design

c) The PCc claim is more pessimistic when a reduced number of defined techniques are used. This tends to be more realistic in terms of the achievable full DC claim in the final design as reliance is placed on limited techniques which must be fully implemented. This may prove difficult to achieve in practice. For example, the theoretical maximum claim may be 99% but in practice, the engineers are only comfortable claiming 95% due to design difficulties. In this case the pessimistic PCc claim would be more accurate.

d) The PCc claim is more optimistic when multiple techniques are used for a failure mode. In practice, multiple techniques can be, and often are, employed in the final design. If one technique proves difficult to implement to 99% and only achieves say 95% then more reliance can be placed on another technique referenced in the PCc conceptual stage. If this second technique only achieved 95% when 99% was required it is still likely that a claim (requires justifiable evidence) of 99% can be made due to the combination of the two techniques providing different diagnostic methods which overall provide the diagnostic coverage required.

A Confidence Table (**CT**) is used, which is effectively a lookup (Table 27).

Table 27: Confidence Table Lookup

$\left[\frac{\sum ATU}{\sum TTA}\right]$ (see '(16)')	CT
<1/6	97%
>=1 / 6	98%
>=1/3	99%
>=1/2	99.5%
>=2/3	100%

The PCc Confidence Factor (**PCcCF**) can now be calculated (16).

$$\boldsymbol{PCcCF = f(\left[\frac{\sum ATU}{\sum TTA}\right], CT)} \quad \textbf{(16)}$$

Where

$$\boldsymbol{ATU} - number\ of\ Available\ Techniques\ Used$$

$$\boldsymbol{TTA} - Total\ number\ of\ Techniques\ Available$$

$$\boldsymbol{CT} - Confidence\ Table$$

With the above information the PCc Diagnostic Coverage Claim (**PCcDCC**) percentage can now be calculated (17).

$$\boldsymbol{PCcDCC = \sum_{fm=1}^{fm='n'} (MCFMDC\ x\ PCcCF)} \quad \textbf{(17)}$$

Where

$$\boldsymbol{fm} - number\ of\ failure\ modes\ applicable\ to\ the\ element\ classification$$

$$'\boldsymbol{n}' - the\ maximum\ number\ of\ failure\ modes$$

3.7.4.3 Calculation Spread sheet

To automate the calculations and provide a fast route to reference individual techniques deployed in a PCc a spread sheet was developed that allowed the data to be input in terms of the failure rates / failure modes and the techniques used to detect the failure. An example of each of the tables for the elements based on the failure modes discussed in 3.7.3.3 is shown below (Table 28 to Table 38).

The principle for populating the tables is identical in each case. Taking Table 28 as an example for a connection:

1) Fill in the reference, normally 1) is the candidate architecture number and C1 would be connection 1 as used on the system diagram so '1)C1' is architecture 1) conection1 as in this example.
2) Fill in 'Y' in the 'Failure Mode Leads to Violation of Safety Goal' column for each failure mode that needs to be considered.
3) For each failure mode to be considered (selected 'Y' in the step above) populate the 'Failure Mode Distribution' column for each of the failure mode rows. The Top 'Failure Mode Distribution' summation cell will be red if the sum is not 100% and change to green when the distribution totals 100% (as in this example).
4) In the 'Technique from ISO 26262' column select which techniques are used and detail the 'Specific PCc' that will be used. Note that multiple techniques may be used against a single failure mode which will increase the confidence level and lead to a higher PCc claim. Also, more than one PCC may be used against a single failure mode and all should be detailed.
5) As the data is populated the spread sheet will update the Full Claim (the maximum achievable according to BS ISO 26262) and the PCc Claim which is used in the PCc SPFM and LFM spread sheets.

Table 28: Connection Example

Reference	1)C1	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description	Specific PCC
Table 26262-5: 2011		100%	0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262	
			Connection Example					D.2.1.1 Used Failure Detection by on-line monitoring High 99%	0.00%

Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage				Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal					
		Low		Medium	High									
		60%		90%	99%									
Harness including splice and connectors	D.3	Open Circuit	Open Circuit		Open Circuit	20%	0%	0%	y					
					Contact resistance	10%	0%	0%	y					
		Short Circuit to ground	Short Circuit to ground (dc Coupled)		Short Circuit to ground (dc Coupled)	30%	0%	0%	y					
			Short Circuit to Vbat		Short Circuit to Vbat	20%	0%	0%	y					
			Short circuit between neighbouring pins		Short circuit between neighbouring pins	10%	0%	0%	y					
					Resistive drift between pins / signal lines	10%	0%	0%	y					

Table 29: Measurement Example

Reference	1)M1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description / Technique from ISO26262							Specific PCC
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	100.00%	Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	
		Measurement Example								High 99%	Low 60%	High 99%	Medium 90%	High 99%	High 99%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage: Low 60%	Medium 90%	High 99%	Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1 Used	D.2.1.1 Used	D.2.6.1 Used	D.2.6.2 Used	D.2.6.3 Used	D.2.6.4 Used	D.2.6.5 Used	
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	0%	0%	y									
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	0%	0%	y									
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%	y									
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	y									
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y									
			Offsets	Offsets	15%	0%	0%	y									
		Stuck in range	Stuck in range	Stuck in range	15%	0%	0%	y									
			Drift & Oscillation	Drift & Oscillation	10%	0%	0%	y									
									0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%		

Table 30: Transducer Example

Reference	1)T1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Transducer Example								Failure Detection by on-line monitoring	Test Pattern	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Sensor valid range	Sensor Correlation	Sensor rationality Check	Voltage or current control (input)	Voltage or current control (output)	
										High 99%	High 99%	High 99%	Low 60%	High 99%	Medium 90%	Low 60%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1 Used	D.2.6.1 Used	D.2.6.5 Used	D.2.10.1 Used	D.2.10.2 Used	D.2.10.3 Used	D.2.8.1 Used	D.2.8.2 Used	
		Low 60%	Medium 90%	High 99%														
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	0%	0%	y		➤	➤	➤	➤		➤			
			Offsets	Offsets	10%	0%	0%	y		➤	➤	➤	➤	➤	➤			
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y		➤	➤	➤	➤	➤	➤			
				Oscillation	5%	0%	0%	y		➤	➤	➤	➤	➤	➤			
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	y								➤	➤	
			Drift	Drift & Oscillation	20%	0%	0%	y								➤	➤	
				Power Spikes	5%	0%	0%	y								➤	➤	
										0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	

Table 31: Data Example (subset 1)

Reference	1)D1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Data Example								Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes		Sensor valid range		Sensor Correlation		Sensor rationality Check		
										High		High		High		Low		High		Medium		
										99%		99%		99%		60%		99%		90%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	
		Low	Medium	High																		
		60%	90%	99%																		
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%	y		➤		➤		➤		➤				➤		
			Offsets	Offsets	10%	0%	0%	y		➤		➤		➤				➤		➤		
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y		➤		➤		➤				➤		➤		
				Oscillation	4%	0%	0%	y		➤		➤		➤				➤		➤		
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	0%	0%	y														
		Message corruption	Message corruption	Message corruption	2%	0%	0%	y														
		Message Delay	Message Delay	Message Delay	3%	0%	0%	y														
		Message Loss	Message Loss	Message Loss	2%	0%	0%	y														
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	0%	0%	y														
			Resequencing	Resequencing	1%	0%	0%	y														
			Insertion of message	Insertion of message	1%	0%	0%	y														
				Masquerading	1%	0%	0%	y														
										0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		

Table 32: Data Example (subset 2)

Reference	1)D1	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
													Technique from ISO26262									
		100%	0.00%	Limited	0.00%	Limited	100.00%															
Table 26262-5: 2011		Data Example						One-bit hardware redundancy	Multi-bit hardware redundancy	Read back of sent message	Complete hardware redundancy	Inspection using test patterns	Transmission redundancy	Information redundancy	Frame counter	Timeout monitoring	Combination of information Redundancy,frame count and timeout					
								D.2.7.1	D.2.7.2	D.2.7.9	D.2.7.3	D.2.7.4	D.2.7.5	D.2.7.6	D.2.7.7	D.2.7.8	D.2.7.6,7,8					
								Low 60%	Medium 90%	Medium 90%	High 99%	High 99%	Medium 90%	Medium 90%	Medium 90%	Medium 90%	High 99%					
								Used	Used	Used	Used	Used	Used	Used	Used	Used	Used					
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal														
		Low 60%	Medium 90%	High 99%																		
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%	y														
			Offsets	Offsets	10%	0%	0%	y														
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y														
				Oscillation	4%	0%	0%	y														
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	0%	0%	y														
		Message corruption	Message corruption	Message corruption	2%	0%	0%	y														
		Message Delay	Message Delay	Message Delay	3%	0%	0%	y														
		Message Loss	Message Loss	Message Loss	2%	0%	0%	y														
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	0%	0%	y														
			Resequencing	Resequencing	1%	0%	0%	y														
			Insertion of message	Insertion of message	1%	0%	0%	y														
				Masquerading	1%	0%	0%	y														
									0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%					

Table 33: Parameter Example (subset 1)

Reference	1)P1	Failure Mode Distribution			Full Claim		PCc Claim	SG Failure Distribution	Technique Description															Specific PCC
Table 26262-5: 2011		100%			0.00%	Limited	0.00% / Limited	100.00%	Technique from ISO26262															
		Parameter Example							Voltage or current control (input)		Voltage or current control (output)		Watchdog with separate time base without time-window		Watchdog with separate time base and time-window		Logical monitoring of program sequence		Combination of temporal and logical monitoring of program sequences		Combination of temporal and logical monitoring of program sequences with time dependency			
									Low 60%		High 99%		Low 60%		Medium 90%		Medium 90%		High 99%		High 99%			
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage: Low 60%	Medium 90%	High 99%	Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.8.1	Used	D.2.8.2	Used	D.2.9.1	Used	D.2.9.2	Used	D.2.9.3	Used	D.2.9.4	Used	D.2.9.5	Used		
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y	➤		➤													
			Drift	Drift & Oscillation	10%	10%	10%	y	➤		➤													
				Power Spikes	5%	5%	5%	y	➤		➤													
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y					➤		➤		➤		➤		➤			
			dc fault model	dc fault model	5%	5%	5%	y					➤		➤		➤		➤		➤			
				Incorrect frequency	10%	10%	10%	y					➤		➤		➤		➤		➤			
				Period jitter	10%	10%	10%	y					➤		➤		➤		➤		➤			
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%	y																
			dc fault model	dc fault model	5%	0%	0%	y																
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y																
			dc fault model	dc fault model	5%	5%	5%	y																
			soft error model	soft error model	5%	5%	5%	y																
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y																
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y																
				dc fault model	5%	5%	5%	y																
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y																
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%			

Table 34: Parameter Example (subset 2)

Reference	1)P1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	100.00%
		Parameter Example							
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	
		Low 60%	Medium 90%	High 99%					
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y	
			Drift	Drift & Oscillation	10%	10%	10%	y	
				Power Spikes	5%	5%	5%	y	
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y	
			dc fault model	dc fault model	5%	5%	5%	y	
				Incorrect frequency	10%	10%	10%	y	
				Period jitter	10%	10%	10%	y	
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%	y	
			dc fault model	dc fault model	5%	0%	0%	y	
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y	
			dc fault model	dc fault model	5%	5%	5%	y	
			soft error model	soft error model	5%	5%	5%	y	
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y	
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y	
				dc fault model	5%	5%	5%	y	
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y	

Technique Description – Technique from ISO26262

Technique	Code	Coverage	Applies to	Used	Total
Parity bit	D.2.5.2	Low 60%	Non-volatile Memory		0.00%
Memory monitoring using error-detection-correction codes (EDC)	D.2.4.1	High 99%	Non-volatile Memory		0.00%
Modified checksum	D.2.4.2	Low 60%	Non-volatile Memory		0.00%
Memory signature	D.2.4.3	High 99%	Non-volatile Memory		0.00%
Block replication (for example double memory with hardware or software comparison)	D.2.4.4	High 99%	Non-volatile Memory		0.00%
RAM Pattern test	D.2.5.1	Medium 90%	Volatile Memory		0.00%
RAM March test	D.2.5.3	High 99%	Volatile Memory	y / y / y	0.00%
Parity bit	D.2.5.2	Low 60%	Volatile Memory		0.00%
Memory monitoring using error-detection-correction codes (EDC)	D.2.4.1	High 99%	Volatile Memory		0.00%
Block replication (for example double memory with hardware or software comparison)	D.2.4.4	High 99%	Volatile Memory		0.00%
Running checksum/CRC	D.2.5.4	High 99%	Volatile Memory		0.00%

Specific PCC

Table 35: Parameter Example (subset 3)

Reference	1)P1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description											
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262											Specific PCC
		Parameter Example								Self-test by software	Self-test by software cross exchanged between two independent units	Self-test supported by hardware (one-channel)	Software diversified redundancy (one hardware channel)	Reciprocal comparison by software in separate processing units	HW redundancy (e.g. Dual Core Lockstep, asymmetric redundancy, coded processing)	Configuration register test	Stack over/under flow detection	Integrated hardware consistency monitoring	Self-test by software	Self-test supported by hardware (one-channel)	
										Medium 90%	Medium 90%	Medium 90%	High 99%	High 99%	High 99%	High 99%	Low 60%	High 99%	Medium 90%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage: Low 60%	Medium 90%	High 99%	Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.3.1 Used	D.2.3.3 Used	D.2.3.2 Used	D.2.3.4 Used	D.2.3.5 Used	D.2.3.6 Used	D.2.3.7 Used	D.2.3.8 Used	D.2.3.9 Used	D.2.3.1 Used	D.2.3.2 Used	
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y													
			Drift	Drift & Oscillation	10%	10%	10%	y													
				Power Spikes	5%	5%	5%	y													
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y													
			dc fault model	dc fault model	5%	5%	5%	y													
				Incorrect frequency	10%	10%	10%	y													
				Period jitter	10%	10%	10%	y													
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%	y													
			dc fault model	dc fault model	5%	0%	0%	y													
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y													
			dc fault model	dc fault model	5%	5%	5%	y													
			soft error model	soft error model	5%	5%	5%	y													
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y													
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y													
				dc fault model	5%	5%	5%	y													
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y													
										0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	

Failure Mode Distribution			Full Claim	PCc Claim		Technique Description Technique from ISO26262				Specific PCC
100%			0.00%	0.00%						
Measure and Report Isolation Resistance Candidate Architecture 1						Voltage or current control (input) Low 60%		Voltage or current control (output) High 99%		
Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	D.2.8.1	Used	D.2.8.2	Used	
Low	Medium	High								
60%	90%	99%								
Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	50%	0%	0%					
	Drift	Drift & Oscillation	20%	0%	0%					
		Power Spikes	30%	0%	0%					
						0.00%		0.00%		

Table 36: PSU Example

Table 37: Output Example

Reference	1)O1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
									Technique from ISO26262														
Table 26262-5: 2011		100%		0.00%	Limited	0.00%	Limited	100.00%	Failure Detection by on-line monitoring			Voltage or current control (input)			Voltage or current control (output)			Failure Detection by on-line monitoring			Test Pattern			Monitoring			
		Outpuit Example							D.2.1.1			D.2.8.1			D.2.8.2			D.2.1.1			D.2.6.1			D.2.11.1		
									Low	60%	Used	Low	60%	Used	High	99%	Used	Low	60%	Used	High	99%	Used	High	99%	Used	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage				Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal																		
		Low		Medium	High																						
		60%		90%	99%																						
Outputs - relays	D.3	Does not energise or de-energise		Does not energise or de-energise	Does not energise or de-energise	20%	0%	0%	y																		
		Welded Contacts		Welded Contacts	Welded Contacts	5%	0%	0%	y																		
				Individual welded contacts	Individual welded contacts	10%	0%	0%	y																		
Power supply	D.9	Under and Over Voltage		Under and Over Voltage	Under and Over Voltage	10%	0%	0%	y																		
				Drift	Drift & Oscillation	15%	0%	0%	y																		
					Power Spikes	5%	0%	0%	y																		
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary		No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	10%	0%	0%	y																		
					Incorrect action	15%	0%	0%	y																		
					Delayed Action	10%	0%	0%	y																		
										0.00%			0.00%			0.00%			0.00%			0.00%			0.00%		

Table 38: Actuator Example

Reference	1)A1	Failure Mode Distribution				Full Claim		PCc Claim	Limited	SG Failure Distribution	Technique Description																
Table 26262-5: 2011		100.00%				0.00%	Limited	0.00%		100.00%	Technique from ISO26262																Specific PCC
		Actuator Example									Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		
											Low		High		Medium		High		High		High		Low		High		
											60%		99%		90%		99%		99%		99%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim			Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																							
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	15%	0%	0%			y	➤		➤		➤		➤		➤		➤						
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%			y	➤		➤		➤		➤		➤		➤						
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%			y	➤		➤		➤		➤		➤		➤						
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%			y	➤		➤		➤		➤		➤		➤						
			Offsets	Offsets	5%	0%	0%			y	➤		➤		➤		➤		➤		➤						
		Stuck in range	Stuck in range	Stuck in range	10%	0%	0%			y	➤		➤		➤		➤		➤		➤						
				Drift & Oscillation	5%	0%	0%			y	➤		➤		➤		➤		➤		➤						
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	5%	0%	0%			y													➤		➤		
			Drift	Drift & Oscillation	20%	0%	0%			y													➤		➤		
				Power Spikes	5%	0%	0%			y													➤		➤		
											0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		

 A.R. Williams

The spreadsheet runs visual basic macros to process the data.

The macro determines both:

1) The maximum diagnostic coverage that can be claimed in a full analysis (i.e. on the final design circuit diagram) which is shown in the tables as the 'Full Claim'.
2) The maximum diagnostic coverage that can be claimed when performing the PCc analysis. This is shown in the tables as the 'PCc Claim'. This is a slightly more conservative value as it is biased by the number of techniques that are used against each failure mode with each additional technique increasing the confidence level. This approach is more realistic of final designs where, typically, a number of different techniques are used to diagnose failures.

The table also refers to the associated techniques from BS ISO26262 part 5 (BSI, 2011e). This is relevant, as it starts to develop the specific requirements that will be carried forward into the detailed design stages.

The steps in the macro are:

1) Determine which failure modes can violate the safety goal. If the failure mode does not violate the safety goal, then it is not included in the diagnostic coverage calculation
2) Confirm that the failure mode distribution percentages for the failure modes that can violate the safety goal add up to 100%, i.e. we have all failure modes covered. This is more of a check to ensure that the engineer has included all relevant data.
3) Determine whether there is a technique available in the safety standard to diagnose each particular failure mode.
4) If a technique is available and the engineer has used it, determine the maximum diagnostic coverage that can be claimed for each implemented technique for each failure mode. This assumes that the planned implementation is in accordance with the robustness required in the standard.
5) For each failure mode, examine each technique used and determine the maximum diagnostic coverage that can be claimed, i.e. if one technique claims 60% diagnostic coverage and one technique 90% coverage then the maximum full claim would be 90%.
6) Examine the failure modes for each of the low, medium and high coverage requirements. For example, if the requirement to claim high diagnostic coverage is that the failure modes of open circuit, contact resistance, short circuit to ground (DC coupled), short circuit to Vbat, short circuit to neighbouring pins and resistive drift between pins all must have diagnostic coverage then a technique must be used to diagnose each of these failure modes. If a

technique is used for each failure mode, then the maximum claim can be up to high (99%). If a technique is not used, then the maximum claim must be lower; in this case the medium claim requirements are checked to ensure a technique exists for each medium failure mode. If a technique is used for each required failure mode, then the maximum claim is limited to medium (90%). If not, then the maximum claim must be lower; in this case the low claim requirements are checked to ensure a technique exists for each low failure mode. If a technique is used, then the maximum claim is limited to low (60%). If not, then the maximum claim is limited to zero (0%), i.e. no coverage.

7) The maximum full claim is worked out from the above two stages. This gives the maximum claim assuming each technique is fully implemented.
8) As the PCc claim is based on a lumped model at the conceptual stage a confidence level (refer to section 3.7.4.2.) is applied to the maximum claim. This is based on the number of techniques that are used against each failure mode as a ratio of the number of techniques that are available in the standard.
9) Finally, the PCc Confidence level is applied (as discussed in 3.7.4.2).

3.7.5 Populating the PCc diagnostic Coverage in the SPFM and LFM Tables

The resultant Maximum PCc claim (calculated using the process described in 3.7.4) is transferred to the SPFM and LFM calculation spreadsheet (for example Table 14) as the diagnostic coverage achieved for the element. Once all elements have their diagnostic coverage values populated the SPFM and LFM for the safety goal achievable for the candidate architecture is calculated.

3.8 Candidate Architectures

The process described in sections 3.5 to 3.7 is repeated for a number of candidate architectures. This is most appropriately achieved iteratively as described in 3.8.1.

3.8.1 Progressive Approach

The method lends itself to a progressive approach:

1) Simple Functional System. The first architecture should satisfy the functional requirements utilising any carry over design as required but with no or only minimal additions for safety. This has the advantage of reducing complexity to a minimum and requires the least amount of effort on the analysis. The outcome of the analysis is a functionally complete design with predicted architectural metrics. The metrics are likely to be much lower in brand new designs than that required for the final design, as safety is not initially included, but they may approach the required targets with carry over designs (which already have safety mechanisms included).

2) Add detection for failure modes that currently have no diagnostic coverage. In analysing the elements in the first architecture proposal it will be obvious in the spread sheet which failure modes have no diagnostic coverage. PCcs are developed that will allow the undiagnosed failures to be detected with as much independence (see 3.8.2) as possible. Repeat the analysis on this new architecture and determine whether the metrics indicate a requirement for further improvement.
3) Add additional detection for failure modes with the lowest diagnostic coverage percentages. This is now an iterative process looking at the failure modes with the lowest diagnostic coverage and applying suitable PCcs to increase diagnostic coverage and review the results of the analysis.
4) Review architectures to see if they can be simplified through decomposition of requirements (see 3.8.3)

By maintaining a progressive approach, the different architectures are documented and quantitatively reviewed as each candidate architecture is completed. This not only allows the design engineer to review the work, but also facilitates discussion with other engineering disciplines. A major advantage of the proposed method is that the architecture designs are simple, the spreadsheets relatively small and they can be discussed with the end customer who has an overview of the whole project. This may identify better solutions early in the project due to improved system understanding and clearly demonstrable PCcs.

It is not necessary to generate a complete new architecture for explorative purposes. A DC percentage can be 'trialled' for an element. For example, elements can be given a fictitious 60%, 90% or 99% claim to see the immediate effect on the SPFM and LFM calculations. This quickly identifies which elements require improvement and gives an idea of the target diagnostic coverage required.

3.8.2 Independence in PCcs

Rather than adding in a disproportionate amount of failure mode detection on a single component / building block, it is beneficial to explore methods of detecting the fault using diverse techniques or techniques that use independent architectural elements. Independent elements may provide a level of redundancy and can be advantageous when applying BS ISO 26262 as it supports requirements decomposition (see 3.8.3). The term independent has a specific meaning within the scope of BS ISO 26262. Generally, independence reduces CCFs and is also helpful in reducing the random hardware failure rate by introducing AND gates into the fault tree analysis used to calculate the random hardware failure rate for the safety goal. This process would be most efficient using a model-based tool such as HiP-HOPS (HiP-HOPS, 2017).

This work is concerned with the architectural metric calculations only. It is interesting that when analysing diagnostic coverage against lumped models, any failure mode with a diagnostic coverage of zero is likely to be a single point failure when the random hardware failures are analysed. The SPFM for the overall architecture may satisfy a particular ASIL level, but any failure modes with 0% or low percentage diagnostic coverage are likely to fail the probabilistic metric for random hardware failure when this analysis is performed (this analysis is not within the scope of the proposed method).

To be independent, all the dependant failures must be analysed to provide evidence that sufficient independence exists or that the potential common causes lead to a safe state. BS ISO 26262 part 1 (BSI, 2011a) defines a dependant failure as single events or single causes that can bypass or invalidate a required independence or freedom from interference between given elements and violate the safety goal. The dependant failure analysis would need to examine similarities between redundant elements i.e. common microcontrollers or common power supplies, functionality implemented with identical software elements, functions and safety mechanism, memory partitioning in microcontrollers, physical separation between elements etc.

Freedom of interference analysis requires examination of cascading failures. A cascading failure in a QM or low ASIL component can cause another component to fail (which has a higher ASIL) and leads to the violation of the safety goal.

By designing the system as proposed in this method the independence between elements is easily depicted in the diagrams. An example of this is shown in section 4.2 and Figure 15 is a typical example where a timing monitor is moved to the battery String (a series connection of battery modules) which provides an independent clock source to that of the Isolation Monitor. Although it is not the rigorous proof required under BS ISO 2626 (BSI, 2011e) it does encourage allocation of PCcs across independent ECUs or hardware architectural elements at the concept stage which gives the design a sound basis for the safety case argument.

For example, when monitoring a single cell in a battery that consists of 12 cells, often a great deal of diagnostics is placed at the cell level; additional monitoring at the cell level for open circuit detection, ADC accuracy checks etc. whereas it may be possible to measure the voltage across all 12 cells using a separate ADC (a PCc) and compare this to the sum of the individual cells and use this to check that the cell voltage reading is correct. It is possible, that one cell can increase by 0.5V and one cell decrease by 0.5V so that the sum remains the same, but if cells are being discharged or charged then the cell voltages should all be varying in the same direction (monotonic) and so an additional

check (another PCc in software proving the sign of the change in voltage with respect to time, a rate monitor or a monotonicity flag) can be designed without the need for additional hardware.

3.8.3 Requirements Decomposition

BS ISO 26262 part 9 (BSI, 2011) allows for 'Requirements decomposition with respect to ASIL tailoring' meaning that safety requirements can be implemented in independent architectural items / elements. This is an important aspect of the standard that can lower the ASIL assigned to decomposed requirements and subsequently reduce the level of rigour required in the development and implementation of certain safety requirements. Note: It does NOT reduce the ASIL rating of the safety goal at the vehicle level.

The proposed method analyses the design in terms of PCcs rather than specific, detailed, low level, diagnostic techniques as detailed in the standard BS ISO 26262 part 5 (BSI, 2011e). This tends to spread the diagnostics across different controllers in systems where multiple controllers exist. This can be considered as requirements decomposition. Although requiring further justification as discussed below, it can have major benefits in achieving the safety targets (and other engineering constraints) when considered at this early stage.

Even at this stage, in the concept design, it is possible to examine the candidate architectures and the allocation of PCcs to the different architectural elements and think about requirements decomposition. High level system requirements with a high ASIL target may be decomposed.

The full details of decomposition are provided in BS ISO 26262 part 9 section 5.4 (BSI, 2011). As an example, the decomposition of an ASIL D requirement taken from the standard is shown below.

An ASIL D requirement shall be decomposed as one of the following:

1) One ASIL C(D) requirement and one ASILA(D) requirement, or
2) One ASIL B(D) requirement and one ASIL B(D) requirement, or
3) One AISL D(D) requirement and one QM(D) requirement

Additional constraints are also placed on the design to ensure that overall safety is not compromised through incorrect application of requirements decomposition.

When decomposing requirements, the associated safety mechanism should be assigned to the highest level ASIL. This is logical, as in general, the safety mechanisms are less complex than the control system that they are diagnosing and achieving a higher ASIL on a simpler system is less onerous than on a complex system.

The proposed method is an important route to facilitate decomposition. Often companies work in isolation when working on different systems, by performing this level of analysis at the concept stage accelerates discussion about decomposition across independent systems very early in the project. This can often lead to lower cost, simpler solutions with equivalent or improved safety by companies working together using decomposition to achieve a better final system design. With the ability to provide predicted architectural metrics for candidate architectures, discussions can take place between suppliers to ensure that data is available to allow PCcs to be implemented. Without this discussion, the OEM tends to dictate the higher ASIL levels (prior to decomposition) to all suppliers and each delivers an individual solution that meets the requirements. This tends to lead to higher costs associated with the rigour achieved in achieving the higher ASIL target. It is recommended to have this discussion prior to formalising the DIAs between the OEM and the suppliers.

The fact that the candidate architectures explore different solutions leads onto exploration of decomposition options early in the design process. This is where the standard intended decomposition to be performed – 'Requirements Decomposition'. One tool that specifically looks at this is discussed by Azevedo (Azevedo LdS, 2014).

3.8.4 Candidate Selection

The method proposed allows all architectures to be considered very quickly to determine the best in terms of architectural metrics. In parallel, a simple cost analysis would provide an indication of the final hardware costs for each architecture. This allows sound engineering decisions to be made early in the design process.

There will be several safety goals and a number of candidate architectures for each safety goal. Generally, experience shows that the candidate architectures, even though designed for different safety goals, tend to lead to a common architecture that can achieve the architectural metrics without over engineering (in terms of component cost and design cost).

In some cases, there can be a conflict between the safety goals. For example, consider the two safety goals:

1) Maintain the cells within their safe operating region for voltage.
2) Ensure torque is delivered as demanded by the driver.

In the first case the logical route is to say that if the cell voltage is too low (over discharged), the control system will limit the charge that can be taken from the cells and ultimately open the contactors to prevent further discharge of the cells. For the second safety goal the control system

should not open the contactors as this would prevent the vehicle management system from delivering the correct torque as demanded by the driver. Practically the first safety goal carries a higher risk and so higher ASIL rating than the second which can be mitigated by driver warnings when the battery is very low on charge (but prior to opening contactors). This difference in ASIL's provides sufficient scope to allow the correct architecture to be chosen and achieve the required ASIL for both safety goals with the same architectural solution.

The candidate architecture diagrams will also show a level of independence which justifies ASIL requirements decomposition as discussed in 3.8.3. In a full design to a functional safety standard it must be remembered that the architectural metrics only form one part of the argument for a safe system other hardware metrics, software process and metrics etc. must also be applied.

3.9 Method Summary

The proposed method allows many safety critical design architectures to be compared in a quantitative way in order the select the most suitable design to take from concept through to final design. The stages are:

1) Describe the desired system function diagrammatically using existing architectural constraints where relevant, i.e. ECUs in the system that have to be re-used.
2) Select a safety goal to analyse and understand which elements can violate the safety goal if a malfunction occurred.
3) Understand the failure modes applicable to each element in the system that can violate the safety goal of interest.
4) Add in PCcs to detect failures in a progressive manner.
5) Quantify the PCcs for the architecture.
6) Calculate the SPFM and LFM that the quantified PCc will achieve when implemented in the final design.
7) Repeat the above steps '3) to '7)' until the ASIL architectural metric targets can be achieved.

This is in line with the required outcomes set out earlier in this section (3.2). As the method is generic it is possible to apply any architectural metric calculation which is based on failure rates, failure modes and diagnostics coverage. For example, it can be used for single point fault metrics in line with BS ISO 262622 part 5 (BSI, 2011e) or safe fail fractions as in BS EN 61508 part 2 (BSI, 2010).

The limitations in the method are:

- The allocation of failure modes percentages to the different element classifications. This limitation is reduced over time as more examples are completed and designs are based on previous projects.
- A number of assumptions have to be made on the failure rate allocated to the lumped models. Again, as more projects are completed, and standard blocks used for inputs, outputs and communications systems etc. the number of assumptions are reduced and confidence is increased in the failure rates used.
- The method is purely examining the architecture based on architectural metrics and does not cover the over aspects such as violation of safety goals due to random hardware failures which requires FTA.
- The is no optimisation in the design. The full design will need further optimisation using additional techniques. One example is automatic optimisation of system architectures using a model-based design approach such as EAST-ADL and HiP-HOPS (Walker, 2013).

4 Practical Applications with Results

4.1 Introduction

Following the approach outlined in section 3, a complete analysis was performed for a Rechargeable Energy Storage System (RESS). This generated a number of safety goals (further safety goals may be identified depending on a more detailed item definition):

1) The isolation resistance between the high voltage battery and the vehicle chassis shall be monitored and deviations below safe limits reported to the vehicle controller.
2) Cell voltages shall be maintained within their safe operating envelope.
3) Cell temperatures shall be maintained within their safe operating region.
4) Charge currents shall be maintained with their safe operating range.
5) Discharge currents shall be maintained with their safe operating range.

The first two were selected for analysis; isolation resistance measurement and maintaining the cells within their safe operating envelope. The method described in section 3 was applied to the two safety goals and a candidate architecture selected based on the outcome of the method. These are discussed in detail in sections 4.2 and 4.3. Both of these studies related to activities the author was working on.

4.2 Isolation Tester

The Isolation tester is considered without the rest of the vehicle as it is considered as a stand-alone system which can then be applied to any system, as long as the safety goals and associated ASIL, are compatible with, or exceed the application requirements and a cross-check of all hazards demonstrates full coverage. The main function is to Measure the Isolation Resistance (MIR).

4.2.1 Safety Goal

4.2.1.1 Aim – Measure and report the resistance between high voltage and chassis

Whenever a high voltage exists (generally considered > 60V dc) then a shock hazard exists if a person can touch exposed live parts. In all automotive designs, the high voltage is isolated from the chassis, this provides and additional level of fault protection as now the person must locate two exposed points of different potential in order to be at risk of electric shock. However, a single fault can cause the chassis to be connected to one side of the high voltage bus. This now means the person only needs to touch one other point with reference to the chassis to risk electric shock.

By measuring the resistance between the chassis and either side of the HV bus, it is possible to report a warning or fault due to insulation breakdown and ensure persons remain safe even in the presence of a single fault.

4.2.1.2 Safety Goal

The safety goal is:

> **Measure and report the minimum isolation resistance between the High Voltage Bus (HV positive OR HV negative) and the chassis of the vehicle.**

The safety goal is applied purely to the Isolation Tester. Any actions revert to the vehicle supervisory system. Typically, the vehicle action would depend on its operating mode:

1) Charging - would disconnect the HV battery when charging as there is a common connection between the vehicle chassis and the earth connection of the electrical distribution system
2) Driving – warn the driver but allow the current drive cycle to complete. Once parked and the drive cycle stopped (key off) then the battery would disconnect and not connect again until either the isolation test had passed, or a service reset is performed followed by a successful isolation test.

4.2.2 System Description

This system is relatively simple, compared to the more complete BMS system (4.3) and so offers a good introduction to application of the method. The system consists of a measurement input to measure the HV voltage with respect to the chassis connection, a microcontroller to calculate the resistance from the voltage measurements and an interface to communicate the information to the vehicle supervisory controller.

The overall system, before the addition of cross checks and analysis can be seen in Figure 11.

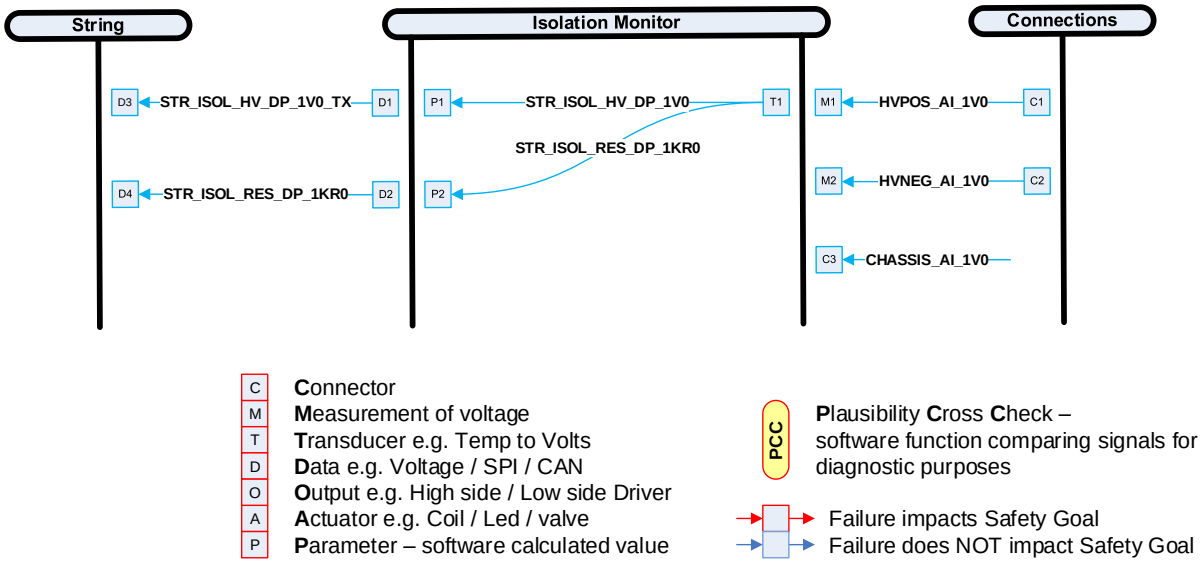


Figure 11: Isolation Tester System Description

4.2.3 Fault Consideration

Based on the system the main faults are incorrect measurement AND / OR incorrect reporting of the measurement value. Either fault can lead to the driver being unaware of a potential hazard.

4.2.4 System Analysis

The system is now analysed to consider which signals are safety critical and the system diagram updated (Figure 12). The HV measurement signal out of the isolation tester is considered as safety critical as other vehicle systems may use this value. By transmitting this along with the resistance value, other systems e.g. the battery management system can rely on this voltage as being accurate and may use it in external plausibility checks.

In theory the isolation tester can generate the warning and fault flags internally and provide these as digital outputs. This has not been considered in this application as the battery management system can achieve a high ASIL due to the microcontroller employed in the design and so it is preferable to use the isolation tester as an intelligent transducer but try and maintain as low a cost as possible while still maintaining the integrity of the overall system.

Should later applications need the warning and fault monitoring in the isolation tester then these outputs can be added either over CAN or hardwired and a new architectural metric design completed by applying the proposed PCc method. This is a good example of an application of this method when examining large systems i.e. array of systems where there is considerable interaction at the interfaces and a number of safety requirements placed on one system from another system; all of which require architectural metrics to be considered early on in the design process.

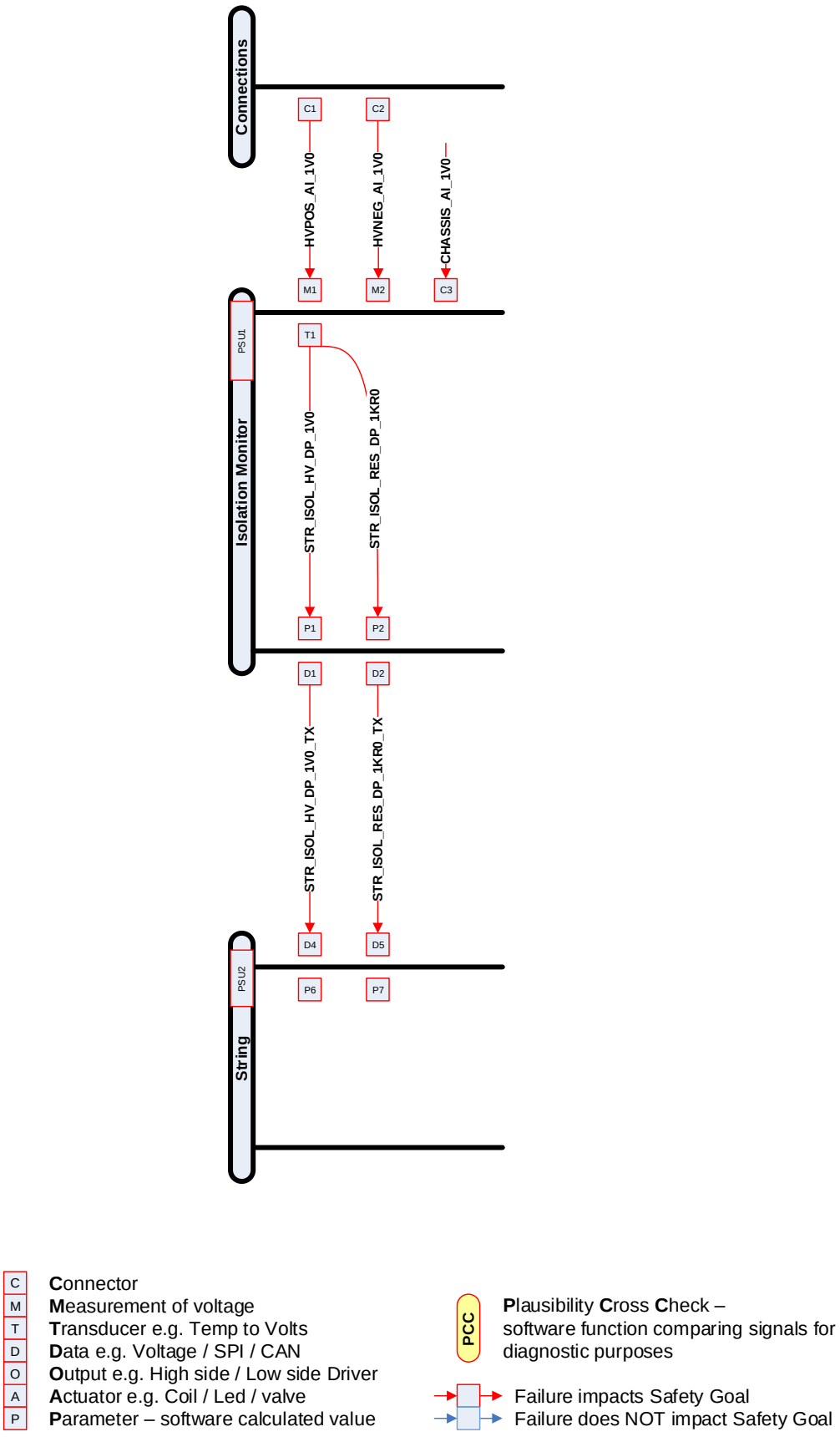


Figure 12: Measure Isolation Resistance – System Diagram with Safety Critical Signals

4.2.5 Candidate Selection

As per the proposed method a candidate architecture is chosen that fulfils the functional requirements and the safety concept without significant emphasis on how the diagnostics will be achieved. This concept is usually relatively simple and low cost and allows the initial data for analysis to be collected.

The selection process for this example starts with a relatively simple software control based concept, then adds reference windows followed by a self-test option followed by a level of independence on the self-test.

4.2.5.1 Measure Isolation Resistance – Architecture 1

The system measures the isolation resistance according to the method described in the United Nations Economic Commission for Europe (UNECE) guideline for 'Uniform provisions concerning the approval of vehicles with regard to specific requirements for the electric power train' (UN ECE Reg 100, 2013).

To sequence the measurements and interpret the voltage measurements into a resistance value, many calculations are required lending itself to the inclusion of a microcontroller in the system. This has the associated ancillaries such as crystal and power supply. The power supply is referenced to the vehicle chassis to make the measurements. In this case, the communications method is over CAN bus so that it can directly link to a suitable CAN bus within the Battery Management System (BMS) or the vehicle CAN bus if no private battery bus is available. The initial architecture is identical to that shown in Figure 12.

4.2.5.2 Measure Isolation Resistance – Architecture 1 Classified Signals

To perform the analysis, many signals are defined which are connected between the critical elements. For clarity, only signals for this candidate architecture diagram (Figure 12) are discussed in this section. The relevant PCcs that are applied are discussed in subsequent sections.

The signals are described as they appear in the architecture diagram (Figure 12) from top left to bottom right.

4.2.5.2.1 Connections

4.2.5.2.1.1 C1, M1 - HVPOS_AI_1V0

The connection to the positive side of the HV bus used for voltage measurements with respect to the chassis connection (C3 - CHASSIS_AI_1V0).

4.2.5.2.1.2 C2, M2 - HVNEG_AI_1V0

The connection to the negative side of the HV bus used for voltage measurements with respect to the chassis connection (C3 - CHASSIS_AI_1V0).

4.2.5.2.1.3 C3 - CHASSIS_AI_1V0

The main reference point for the measurements. This is assumed to be a separate connection to that of the 0V of the 12V power supply.

4.2.5.2.2 Isolation Tester Inputs

4.2.5.2.2.1 T1, P1 - STR_ISOL_HV_DP_1V0

The measurement is a voltage measurement at the front end but in order to meet accuracy requirements the concept includes an amplifier / buffer in order to be able to control the gain of the measurement circuit which is why the element is classed as a transducer.

4.2.5.2.2.2 T1, P2 - STR_ISOL_RES_DP_1KR0

The transducer also provides all the necessary scaled measurements for the resistance calculation in the microcontroller. This is converted to an internal parameter (resolution 1kR) which is then used to generate the necessary data for the CAN interface.

4.2.5.2.3 Isolation Tester Outputs

CAN will be updated periodically depending on the measurement rate in the isolation tester. Typically, 100ms update rates on CAN are sufficient for isolation resistance values as measurements take in excess of 500mS. Additional information such as status or voltage for diagnostic purposes for other systems which can be included in the same data packet for the message may require a faster update rate.

4.2.5.2.3.1 D1, D4 - STR_ISOL_HV_DP_1V0_TX

The voltage measurement values transmitted by the isolation tester.

4.2.5.2.3.2 D2, D5 - STR_ISOL_RES_DP_1KR0_TX

The measured isolation resistance value transmitted by the isolation tester.

4.2.5.3 Measure Isolation Resistance – Architecture 1 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.2.5.4. Table 39 acts as a cross reference into the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 39: MIR Architecture 1 Element Cross Reference to Diagnostic Coverage Claims

Element	Diagnostic Coverage Calculation Table Reference in Appendix D1 – MIR – Architecture 1 DC% Claims
1)C1	Table 80: MIR – Architecture 1 Connection 1
1)C2	Table 81: MIR – Architecture 1 Connection 2
1)C3	Table 82: MIR – Architecture 1 Connection 3
1)D1	Table 83: MIR – Architecture 1 Data 1 (subset 1) Table 84: MIR – Architecture 1 Data 1 (subset 2)
1)D2	Table 85: MIR – Architecture 1 Data 2 (subset 1) Table 86: MIR – Architecture 1 Data 2 (subset 2)
1)D4	Table 87: MIR – Architecture 1 Data 4 (subset 1) Table 88: MIR – Architecture 1 Data 4 (subset 2)
1)D5	Table 89: MIR – Architecture 1 Data 5 (subset 1) Table 90: MIR – Architecture 1 Data 5 (subset 2)
1)M1	Table 91: MIR – Architecture 1 Measurement 1
1)M2	Table 92: MIR – Architecture 1 Measurement 2
1)P1	Table 93: MIR – Architecture 1 Parameter 1 (subset 1) Table 94: MIR – Architecture 1 Parameter 1 (subset 2) Table 95: MIR – Architecture 1 Parameter 1 (subset 3)
1)P2	Refer to 1)P1 as similar techniques used
1)P4	Refer to 1)P1 as similar techniques used
1)P6	Refer to 1)P1 as similar techniques used
1)PSU1	Table 96: MIR – Architecture 1 Power Supply 1
1)PSU2	Refer to 1)PSU1 as similar techniques used
1)T1	Table 97: MIR – Architecture 1 Transducer 1

4.2.5.3.1 Element 1)C1, 1)C2, 1)C3

No diagnostic coverage is provided for these connections.

4.2.5.3.2 Element 1)D1, 1D2, 1)D4,1)D5

Only the data failure modes of this signal are covered and the normal Data PCCs are used – see 4.2.5.4.1.

4.2.5.3.3 Element 1)M1, 1)M2

No diagnostic coverage is provided for these measurements.

4.2.5.3.4 Element 1)P1, 1)P2, 1)P4, 1)P6

A number of standard Parameter PCcs are performed as covered in section 4.2.5.4.3.

4.2.5.3.5 Element 1)PSU1, 1)PSU2

PCc_PSU_MON monitors all power supply faults (4.2.5.4.4).

4.2.5.3.6 Element 1)T1

PCc_PSU_MON (4.2.5.4.4) is used for the power supply section; however there is no coverage for the remaining measurement functionality.

4.2.5.4 Measure Isolation Resistance – Architecture 1 Plausibility Cross checks

Several generic PCcs are used in this design relating to power supply monitoring, data communications and internal microcontroller functionality. These are discussed below based on the element classifications.

4.2.5.4.1 Data

The microcontroller is responsible for calculating transmission checksums (PCc_Data_Checksum), frame sequence counters (PCc_Frame_Seq / PCc_Frame_Count) and transmission timing (PCc_Poll_Response_Time) of data. To ensure end to end data integrity it is the responsibility in the higher software layers (application) to pack the data with rolling counts and checksums. Additionally, checks performed in the CAN stack are to ensure data to be transmitted is correct (i.e. no corruption has occurred between the application software and the point of transmission) and also monitor poll / response timing.

4.2.5.4.1.1 PCc_Data_Checksum

A data checksum can be performed in many ways. This may be a simple parity check, and exclusive-OR check or a more complicated Cyclic Redundancy Check (CRC). The integrity of the check is based on the criticality of the data as described in each of the individual element references. The integrity can also be improved based on the position of the checksum calculation in the data timeline. The higher the integrity the higher the diagnostic coverage achievable. The preferred method is to use an end-to-end checksum whereby the data is packed in the application with the calculated checksum to form a high integrity data packet. The data is unpacked by the application at the receiving end and verified using the same checksum calculation us used by the transmitting application. This eliminates any errors in data processing through CAN stacks and other lower levels of software. To a certain extent it also protects against timing issues as the data can be packed in a function call that provides the data and unpacked in a function that utilises the data.

This PCc does not only apply to data passed over a communications networks, such as CAN, it can also be applied to critical data packets, for example data passed between algorithms or state machines within a single microcontroller if necessary.

4.2.5.4.1.2 PCc_Frame_Seq / PCc_Frame_Count

Data frames sent between ECUs generally contain live data which should be processed in the correct order. This means that the ECU receiving the data needs to know the order in which the data was sent (normally there is no specific timestamp with a CAN protocol) a combination of the frame sequence (sometimes referred to as a rolling counter) and independent monitoring of the timing is used.

4.2.5.4.2 PCc_Poll_Response_Time

Individual message poll and response timing checked by the receiving ECU. For example, if a periodic message is expected to be transmitted every 20mS then the receiving ECU can reset a timer when the message is received and then increment the timer until the next valid message is received. The time difference measured between the two messages can be compared to the correct time of 20mS and the ECU can determine whether the message is being received at a higher rate or lower rate than expected. As CAN traffic is not deterministic, a certain timing tolerance would be allowed. It is important that CAN bus loading is appropriate to provide bus access meaning that time delays can be accommodated without causing nuisance trips. If a message is lost (no longer present on the bus) the receiving ECU will have to decide whether to use data from the last known good message or else revert to default data.

4.2.5.4.3 Parameters

The microcontroller performs many standard tests. This is kept relatively general for each PCc, but each test would be developed when working with a specific microcontroller in the final design. Many microcontrollers have a range on Built in Self-Test (BIST) functions that cover as a minimum all the PCcs discussed here plus additional ones that are more specific to the peripherals on the microcontroller. The Texas Instruments Hercules series (Texas Instruments, 2014) is a good example of microcontrollers specifically designed for use in safety critical applications and there is sufficient data available in the public domain to perform the PCc calculations, more detailed information (as required for final design) is available under NDA.

4.2.5.4.4 PCc_PSU_Mon

Monitoring of the PSU can be achieved in a number of ways with differing integrity levels. The test can be performed by a simple comparator in the microcontroller that can detect brown-out, power dips etc. and inform the application of the type of power transient either as it happens for a very

short transient or after a microcontroller reset for longer power dips. In more complex microcontrollers there may be a companion chip that performs detailed power supply monitoring in conjunction with a watchdog, reset function and in some cases a safety output for disabling output drivers.

4.2.5.4.5 PCc_Code_Seq

The microcontroller will execute all required tasks, either through a Real Time operating System (RTOS), or a simple scheduler. These relate to management of the lower level tasks such as input output control and communication message handling, microcontroller testing such as memory tests, peripheral tests etc. and management of the main application tasks such as state machines and control strategies.

The code sequence check ensures that these tasks are scheduled correctly in terms of the correct order and also that they are performed in a timely manner. This ensures that the tasks are handled in a deterministic way. The sequence check identifies slow or fast tasks or incorrect task sequencing, if faults are detected it can decide to perform some form of soft restart, a soft reset or in extreme cases trip the watchdog which in turn performs a complete hardware reset of the microcontroller. Bearing in mind that this is a safety critical application a soft recovery is preferred to minimise disruption but this may not always be possible.

4.2.5.4.6 PCc_MICRO_Test

Microcontrollers have a number of self-test functions built into them. These can be run at start up or periodically during normal operation. It is the software engineer's responsibility to ensure that these self-tests are executed in a timely manner, results are consistent with correct operation and that any deviation from correct operation is detected and the microcontroller operation managed if a fault is found. As these tests are critical, a test schedule monitor would normally be included as part of the PCc_Code_Seq check. The PCc assumes that all peripherals used by the application and those powered / running are checked. Even a peripheral not used in the application if powered (i.e. not properly disabled) may influence operation of another safety critical function. Normally, peripherals can be disabled through software configuration of the control registers, however, a detailed knowledge of the microcontroller may be required to ensure this is the case.

Normally the data sheets for the microcontroller will specify all peripheral tests available and for microcontrollers designed for use in safety critical applications there is normally sufficient data available to allow the achievable diagnostic coverage to be calculated.

Typical peripherals include:

- Integrated memory – flash, Data RAM, Data flash EEPROM emulation, trace memory.
- Direct memory access to transfer data.
- CAN communication channels.
- Inter-Integrated Circuit communication ports (I^2C).
- Serial Peripheral Interfaces (SPI).
- Universal Asynchronous Receiver Transmitter (UART).
- Timers.
- Analogue to digital converters.
- Pulse Width Modulation (PWM) outputs.
- Input capture and compare units.
- On board temperature sensing.
- Dedicated general purpose input / output pins. Etc.

4.2.5.4.7 PCc_RAM_Test

RAM tests may be scheduled (at start up or cyclically during normal operation) or completed just prior to access to memory and / or just after writing to RAM. This may be a simple parity test, a more complex checksum which is performed by software, or, in higher end microcontrollers, a dedicated memory manager which is used to perform access monitoring of the memory. This may also extend to memory protection which ensures that only the correct functions can read from / write to specific areas of memory. This is a requirement where functions with different ASIL requirements co-exist in the same microcontroller as discussed in BS ISO 26262 part 9 section 6 - Criteria for coexistence of elements (BSI, 2011).

4.2.5.4.8 PCc_NV_Test

Non-Volatile memory tests are normally run at start up and during normal operation to verify any calibration / configuration data that may be set at the end of line or learnt as the application is used (e.g. storage of diagnostic trouble codes or data logging).

4.2.5.5 Measure Isolation Resistance – Architecture 1 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 40 and the LFM calculation shown in Table 41. For presentation purposes the tables are split into two sections (SPFM and LFM) although a single spreadsheet would normally be used.

Table 40: Measure Isolation Resistance Architecture 1 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Safety Critical Failure rate	Failure mode that can violate safety goal w/o safety mechanisms?	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Connections											
HVPOS_AI_1V0	Connection	1)C1	0.0353	y	0.0353	45%	0.0159	y		0.00%	0.0159
HVNEG_AI_1V0	Connection	1)C2	0.0353	y	0.0353	45%	0.0159	y		0.00%	0.0159
Isolation Monitor Inputs											
HVPOS_AI_1V0	Measurement	1)M1	4.9000	y	4.9000	45%	2.2050	y		0.00%	2.2050
HVNEG_AI_1V0	Measurement	1)M2	4.9000	Y	4.9000	45%	2.2050	y		0.00%	2.2050
CHASSIS_AI_1V0	Connection	1)C3	0.0353	Y	0.0353	45%	0.0159	y		0.00%	0.0159
Isolation Monitor Internal											
STR_ISOL_HV_1V0 STR_ISOL_RES_DP_1KR0	Transducer	1)T1	14.3674	Y	14.3674	45%	6.4653	y	PCc_PSU_MON	0.00%	6.4653
STR_ISOL_HV_1V0	Parameter	1)P1	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.02%	0.1197
Power Supply	General - PSU	1)PSU1	12.0000	Y	12.0000	45%	5.4000	y	PCc_PSU_MON	98.51%	0.0807
Isolation Monitor Outputs											
STR_ISOL_HV_DP_1V0_TX	Data	1)D1	3.9991	Y	3.9991	45%	1.7996	y	PCc_DATA_CHECKSUM, PCc_FRAME_COUNT, PCc_POLL_RESPONSE_TIME	0.00%	1.7996
String Inputs											
STR_ISOL_HV_DP_1V0_TX	Data	1)D4	3.9991	Y	3.9991	45%	1.7996	y	PCc_DATA_CHECKSUM, PCc_FRAME_COUNT, PCc_POLL_RESPONSE_TIME	0.00%	1.7996
String Internal											
STR_ISOL_HV_DP_1V0_TX	Parameter	1)P6	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.02%	0.1197
Power Supply	General - PSU	1)PSU2	12.0000	Y	12.0000	45%	5.4000	y	PCc_PSU_MON	98.51%	0.0807
Total FR (FIT)			**74.115**		**74.115**						**14.923**
									Single Point Fault Metric		**79.9%**

Table 41: Measure Isolation Resistance Architecture 1 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Element reference	Failure Mode coverage with respect to Latent failures, %	Latent.multiple-Point failure rate/FIT
Connections											
HVPOS_AI_1V0	Connection	1)C1	0.0353	y	0.0353	0	Y	SC_EXT_REF		90%	0.0000
HVNEG_AI_1V0	Connection	1)C2	0.0353	y	0.0353	0	Y	SC_EXT_REF		90%	0.0000
Isolation Monitor Inputs											
HVPOS_AI_1V0	Measurement	1)M1	4.9000	y	4.9000	0	Y	SC_EXT_REF		90%	0.0000
HVNEG_AI_1V0	Measurement	1)M2	4.9000	Y	4.9000	0	Y	SC_EXT_REF		90%	0.0000
CHASSIS_AI_1V0	Connection	1)C3	0.0353	Y	0.0353	0	Y	SC_EXT_REF		90%	0.0000
Isolation Monitor Internal											
STR_ISOL_HV_1V0 STR_ISOL_RES_DP_1KR0	Transducer	1)T1	14.3674	Y	14.3674	0	Y	SC_EXT_REF		90%	0.0000
STR_ISOL_HV_1V0	Parameter	1)P1	8.9218	Y	8.9218	3.89505607	Y	Wdog		60%	1.5580
Power Supply	General - PSU	1)PSU1	12.0000	Y	12.0000	5.31927	Y	Wdog		60%	2.1277
Isolation Monitor Outputs											
STR_ISOL_HV_DP_1V0_TX	Data	1)D1	3.9991	Y	3.9991	0					
String Inputs											
STR_ISOL_HV_DP_1V0_TX	Data	1)D4	3.9991	Y	3.9991	0					
String Internal											
STR_ISOL_HV_DP_1V0_TX	Parameter	1)P6	8.9218	Y	8.9218	3.89505607	Y	Wdog		60%	1.5580
Power Supply	General - PSU	1)PSU2	12.0000	Y	12.0000	5.31927	Y	Wdog		60%	2.1277
Total FR (FIT)			**74.115**		**74.115**						**7.371**
										Latent Fault metric	**87.5%**

The PCc architectural analysis results in a SPFM of 79.9% (Table 40) and a LFM of 87.5% (Table 41). This means the design is not capable of achieving ASIL B (the first ASIL level that requires architectural metric analysis). Significantly, there are effectively several single point failures – i.e. no diagnostic coverage on safety critical components. Although the SPFM for the overall architecture is capable of achieving ASIL A, the fault trees used for calculating the probabilistic metric for random hardware failure would highlight this problem.

4.2.5.6 Measure Isolation Resistance – Architecture 2

Improvement can quite easily be made by cross referencing voltage and resistance measurements against windows that can be calibrated to provide an upper and lower value. If they are in a suitable working range, signal plausibility confidence is increased. The updated system diagram is shown in Figure 13.

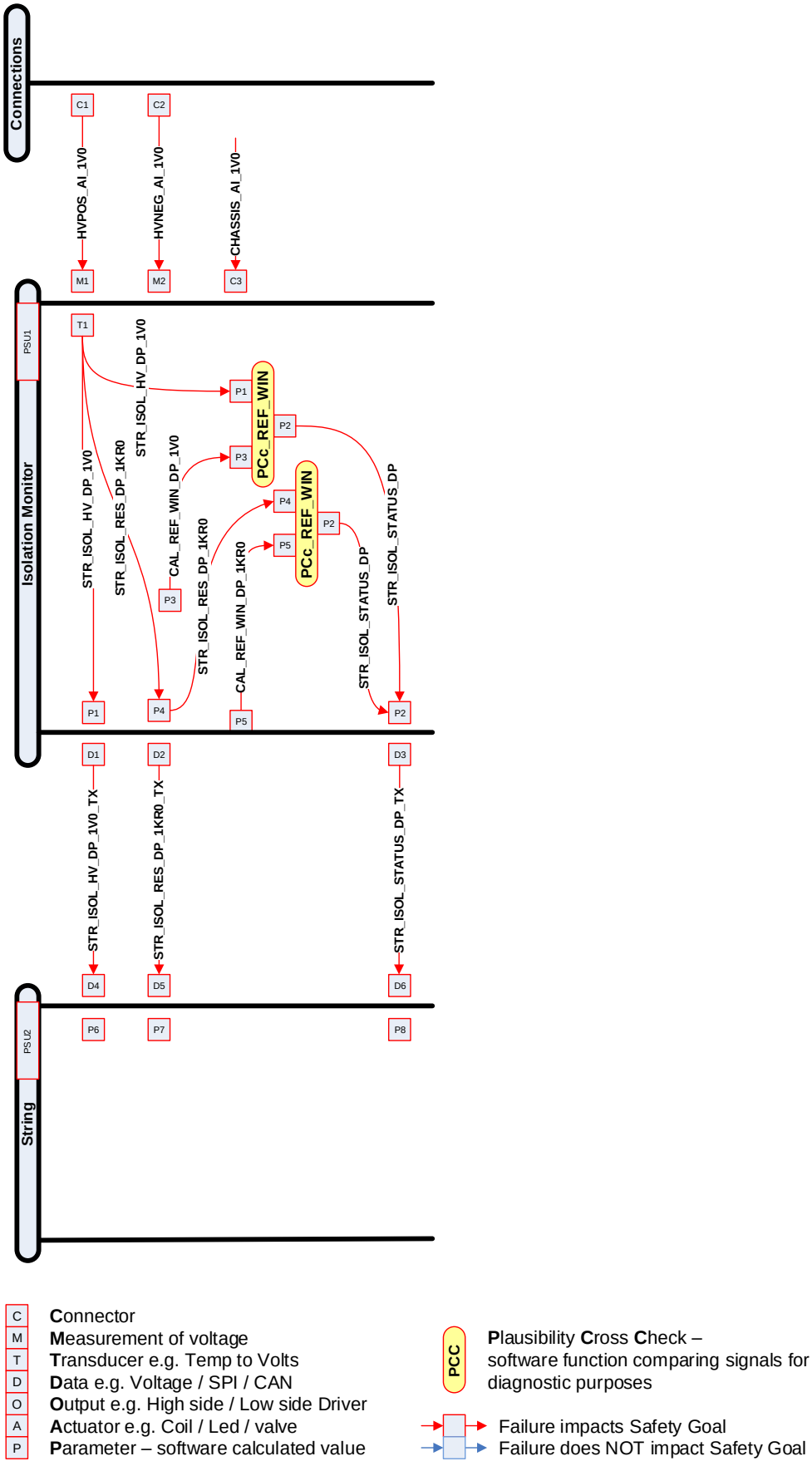


Figure 13: Measure Isolation Resistance – System Diagram - Architecture 2

4.2.5.7 Measure Isolation Resistance – Architecture 2 Classified Signals

The plausibility cross checks require several additional signals. Only new signals for this candidate architecture diagram (Figure 13) are discussed in this section. The relevant PCcs that are applied are discussed in subsequent sections.

The signals are described as they appear in the architecture diagram (Figure 13) from top left to bottom right.

4.2.5.7.1 Isolation Tester Internal Signals

4.2.5.7.1.1 P3 - CAL_REF_WIN_DP_1V0

The calibration value for the reference voltage window.

4.2.5.7.1.2 P5 - CAL_REF_WIN_DP_1KR0

The calibration value for the reference resistance window.

4.2.5.7.1.3 P2 - STR_ISOL_STATUS_DP

The status flag set to show that the measurements are plausible.

4.2.5.7.1.4 D3, D6, P8 - STR_ISOL_STATUS_DP_TX

The status flag transmitted to the string and converted to a parameter for internal use in the string controller.

4.2.5.8 Measure Isolation Resistance – Architecture 2 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.2.5.9. Table 42 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 42: MIR Architecture 2 Element Cross Reference to Diagnostic Coverage Claims

Element	**Diagnostic Coverage Calculation Table Reference in Appendix D2 – MIR – Architecture 2 DC% Claims**
2)C1	Table 98: MIR – Architecture 2 Connection 1
2)C2	Table 99: MIR – Architecture 2 Connection 2
2)D1	Table 100: MIR – Architecture 2 Data 1 (subset 1) Table 101: MIR – Architecture 2 Data 1 (subset 2)
2)D2	Refer to 2)D1 as similar techniques used
2)D3	Refer to 2)D1 as similar techniques used
2)D4	Refer to 2)D1 as similar techniques used

Element	Diagnostic Coverage Calculation Table Reference in Appendix D2 – MIR – Architecture 2 DC% Claims
2)D5	Refer to 2)D1 as similar techniques used
2)D6	Refer to 2)D1 as similar techniques used
2)M1	Table 102: MIR – Architecture 2 Measurement 1
2)M2	Refer to 2)M1 as similar techniques used
2)P3	Table 103: MIR – Architecture 2 Parameter 3 (subset 1) Table 104: MIR – Architecture 2 Parameter 3 (subset 2) Table 105: MIR – Architecture 2 Parameter 3 (subset 3)
2)P5	Refer to 2)P3 as similar techniques used
2)P6	Table 106: MIR – Architecture 2 Parameter 6 (subset 1) Table 107: MIR – Architecture 2 Parameter 6 (subset 2) Table 108: MIR – Architecture 2 Parameter 6 (subset 3)
2)P7	Refer to 2)P6 as similar techniques used
2)P8	Refer to 2)P6 as similar techniques used
2)T1	Table 109: MIR – Architecture 2 Transducer 1

4.2.5.8.1 Element 2)C1, 2)C2

A reference window - PCc_REF_WINDOW (4.2.5.9.1.1) increases diagnostic coverage from 0% to 72%.

4.2.5.8.2 Element 2)D1, 2)D2, 2)D3, 2)D4, 2)D5, 2)D6, 2)M1, 2)M2

The reference window (4.2.5.9.1.1) significantly increases coverage on the Data as there is confidence that the signal is within a valid range.

4.2.5.8.3 Element 2)P3, 2)P5, 2)P6, 2)P7, 2)P8

This architecture employs a number of additional Parameters all of which are covered by the standard Parameter diagnostics (4.2.5.4.3).

4.2.5.8.4 Element 2)T1

The reference window (4.2.5.9.1.1) is now applicable to this input; however, as this is the conversion to resistance, the diagnostic coverage remains at 0% as a number of failure modes are still undiagnosed in terms of the actual resistance value.

4.2.5.9 Measure Isolation Resistance – Architecture 2 Plausibility Cross checks

4.2.5.9.1 Isolation Tester PCCs

4.2.5.9.1.1 PCc_REF_WIN – Reference Window

PCc_REF_WIN takes two inputs – one, a live measurement value and the other a calibration window with an upper and lower limit. The PCc ensures that the measured value is within the window. The output is a status flag to show whether the measured signal is plausible or not. If the measurements are not plausible the string controller (receiver of the signal in this example) can determine a relevant course of action. The reference window would normally be selected to have a lower limit that is greater than the warning limit. This means that the isolation tester is effectively monitoring the warning level as well as the string controller.

4.2.5.10 Measure Isolation Resistance – Architecture 2 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 43 and the LFM calculation shown in Table 44.

Table 43: Measure Isolation Resistance Architecture 2 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure Rate/FIT	Failure rate distribution, %	Safety Critical Failure rate	Failure mode that can violate safety goal w/o safety mechanisms?	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Connections											
HVPOS_AI_1V0	Connection	2)C1	0.0353	y	0.0353	45%	0.0159	y	PCc_Ref_WIN	72.00%	0.0045
HVNEG_AI_1V0	Connection	2)C2	0.0353	y	0.0353	45%	0.0159	y	PCc_Ref_WIN	72.00%	0.0045
Isolation Monitor Inputs											
HVPOS_AI_1V0	Measurement	2)M1	4.9000	y	4.9000	45%	2.2050	y	PCc_Ref_WIN	0.00%	2.2050
HVNEG_AI_1V0	Measurement	2)M2	4.9000	Y	4.9000	45%	2.2050	y	PCc_Ref_WIN	0.00%	2.2050
CHASSIS_AI_1V0	Connection	1)C3	0.0353	Y	0.0353	45%	0.0159	y		0.00%	0.0159
Isolation Monitor Internal											
STR_ISOL_HV_1V0 STR_ISOL_RES_DP_1KR0	Transducer	2)T1	14.3674	Y	14.3674	45%	6.4653	y	PCc_REF_WINDOW	0.00%	6.4653
STR_ISOL_HV_1V0	Parameter	1)P1	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.02%	0.1197
Power Supply	General - PSU	1)PSU1	12.0000	Y	12.0000	45%	5.4000	y	PCc_PSU_MON	98.51%	0.0807
Isolation Monitor Outputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D1	3.9991	Y	3.9991	45%	1.7996	y	PCc_REF_WINDOW	95.89%	0.0740
String Inputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D4	3.9991	Y	3.9991	45%	1.7996	y	PCc_REF_WINDOW	95.89%	0.0740
String Internal											
STR_ISOL_HV_DP_1V0_TX	Parameter	2)P6	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.02%	0.1197
Power Supply	General - PSU	1)PSU2	12.0000	Y	12.0000	45%	5.4000	y	PCc_PSU_MON	98.51%	0.0807
Total FR (FIT)			**74.115**		**74.115**						**11.449**
										Single Point Fault Metric	**84.6%**

Table 44: Measure Isolation Resistance Architecture 2 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure Rate/FIT	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Element reference	Failure Mode coverage with respect to Latent failures, %	Latent.multiple-Point failure rate/FIT
Connections											
HVPOS_AI_1V0	Connection	2)C1	0.0353	y	0.0353	0.0114	Y	SC_EXT_REF		90%	0.0011
HVNEG_AI_1V0	Connection	2)C2	0.0353	y	0.0353	0.0114	Y	SC_EXT_REF		90%	0.0011
Isolation Monitor Inputs											
HVPOS_AI_1V0	Measurement	2)M1	4.9000	y	4.9000	0.0000	Y	SC_EXT_REF		90%	0.0000
HVNEG_AI_1V0	Measurement	2)M2	4.9000	Y	4.9000	0.0000	Y	SC_EXT_REF		90%	0.0000
CHASSIS_AI_1V0	Connection	1)C3	0.0353	Y	0.0353	0.0000	Y	SC_EXT_REF		90%	0.0000
Isolation Monitor Internal											
STR_ISOL_HV_1V0 STR_ISOL_RES_DP_1KR0	Transducer	2)T1	14.3674	Y	14.3674	0.0000	Y	SC_EXT_REF		90%	0.0000
STR_ISOL_HV_1V0	Parameter	1)P1	8.9218	Y	8.9218	3.8951	Y	Wdog		60%	1.5580
Power Supply	General - PSU	1)PSU1	12.0000	Y	12.0000	5.3193	Y	Wdog		60%	2.1277
Isolation Monitor Outputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D1	3.9991	Y	3.9991	1.7256					
String Inputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D4	3.9991	Y	3.9991	1.7256					
String Internal											
STR_ISOL_HV_DP_1V0_TX	Parameter	2)P6	8.9218	Y	8.9218	3.8951	Y	Wdog		60%	1.5580
Power Supply	General - PSU	1)PSU2	12.0000	Y	12.0000	5.3193	Y	Wdog		60%	2.1277
Total FR (FIT)			**74.115**		**74.115**						**7.374**
									Latent Fault metric		**88.2%**

As expected the SPFM has increased, now achieving 84.6% (Table 43) compared to 79.9% (candidate architecture 1). A slight increase in LFM from 87.5% (architecture 1) to 88.2% (Table 44) has also been achieved. Due to the SFM being less than 90%, ASIL B can still not be achieved and the dominant area of concern (due to the PCc claim of 0%) is the isolation measurement and transducer.

4.2.5.11 Measure Isolation Resistance – Architecture 3

To provide evidence that the measurement system is working a self-test system was added. This switches a resistance between one side of the HV Bus voltage (HV Positive or HV Negative) and chassis. In this example HV Negative (HVNEG_AI_1V0) has been chosen. The self-test resistance is chosen so that it can reduce the isolation resistance (as it is effectively in parallel to the existence HV Bus – chassis resistance). The Isolation Tester can then check that the measured resistance is that of the previously measured HV Bus to chassis resistance in parallel with the known self-test resistance value. The updated system diagram is shown in Figure 14 .

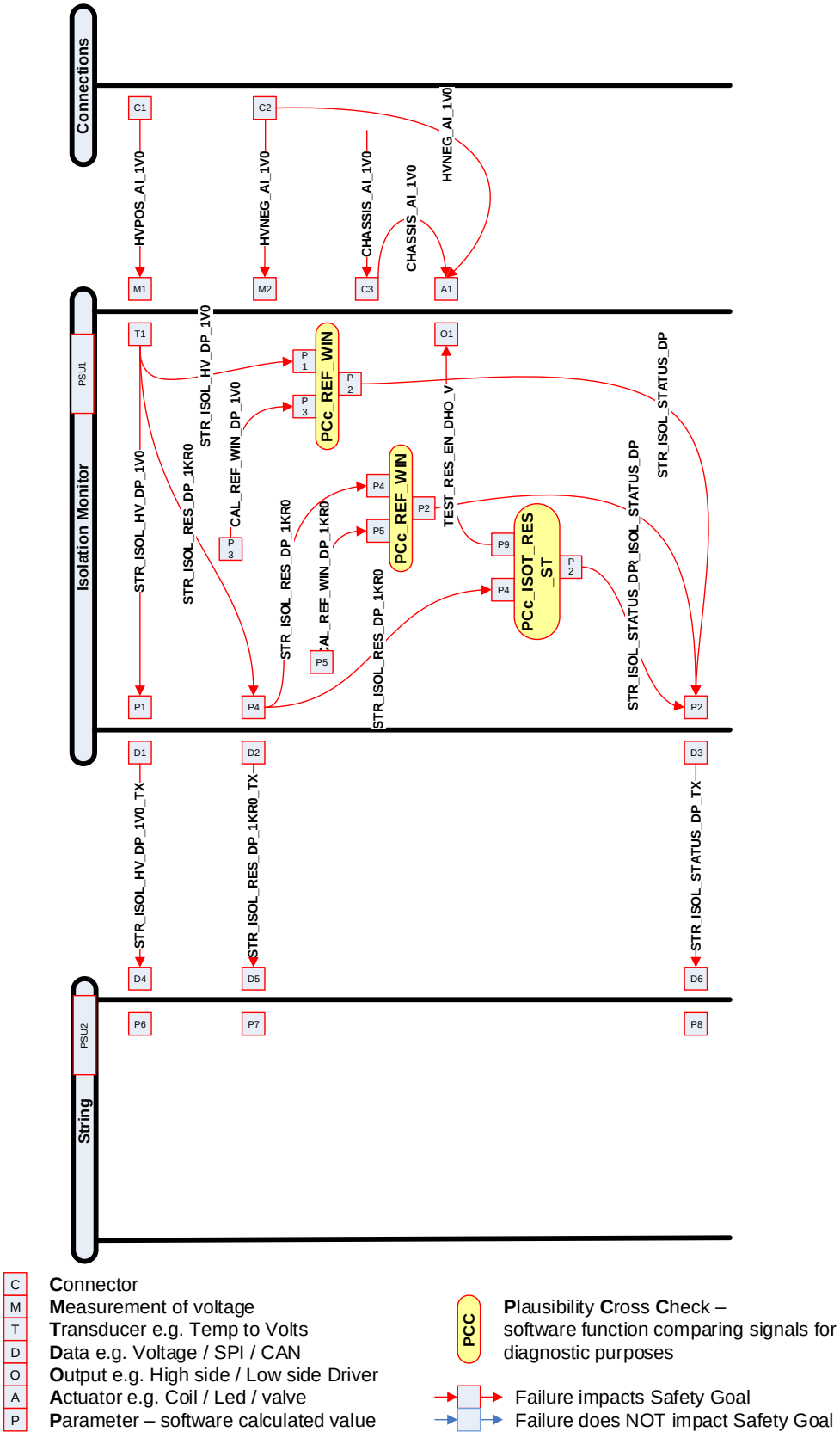


Figure 14: Measure Isolation Resistance – System Diagram - Architecture 3

4.2.5.12 Measure Isolation Resistance – Architecture 3 Classified Signals

To implement the PCc a new signal is added for this candidate architecture diagram (Figure 14). New signals are discussed in this section. The relevant PCcs that are applied are discussed in subsequent sections.

4.2.5.12.1 Isolation Tester Internal Signals

4.2.5.12.1.1.1 P9, O1, A1 - TEST_RES_EN_DHO_V

A high side output (O1) that switches a test resistor between one side of the HV bus and the chassis connection based on a demand from the microcontroller (P9). This would be via a relay (A1).

4.2.5.13 Measure Isolation Resistance – Architecture 3 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.2.5.14. Table 45 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 45: MIR Architecture 3 Element Cross Reference to Diagnostic Coverage Claims

Element	**Diagnostic Coverage Calculation Table Reference in Appendix D3 – MIR – Architecture 3 DC% Claims**
3)A1	Table 110: MIR – Architecture 3 Actuator 1
3)C1	Table 111: MIR – Architecture 3 Connection 1
3)C2	Refer to 3)C1 as similar techniques used
3)C3	Table 112: MIR – Architecture 3 Connection 3
3)D7	Table 113: MIR – Architecture 3 Data 7 (subset 1) Table 114: MIR – Architecture 3 Data 7 (subset 2)
3)D8	Refer to 3)D7 as similar techniques used
3)M1	Table 115: MIR – Architecture 3 Measurement 1
3)M2	Refer to 3)M1 as similar techniques used
3)O1	Table 116: MIR – Architecture 3 Output 1
3)T1	Table 117: MIR – Architecture 3 Transducer 1

4.2.5.13.1 Element 3)A1

A new element added to this architecture for the self-test PCc. The actuator itself is effectively diagnosed by the self-test (4.2.5.14.1.1) and so 73.6% coverage is claimed in this architecture.

4.2.5.13.2 Element 3)C1, 3)C2

The self-test (4.2.5.14.1.1) significantly increases the diagnostic coverage when used in combination with the reference window achieving a claim of 99%.

4.2.5.13.3 Element 3)C3

The self-test (4.2.5.14.1.1) improves the chassis connection diagnostics by 72% because the self-test resistance provides a new path to the chassis connection.

4.2.5.13.4 Element 3)D7, 3)D8

New elements added to the architecture in order to perform the self-test (4.2.5.14.1.1) which as well as being covered by the standard data diagnostics (4.2.5.4.1) are to some extent also covered by the reference window (4.2.5.9.1.1).

4.2.5.13.5 Element 3)M1, 3)M3

An increase of 93.5% is achieved by the addition of the self-test (4.2.5.14.1.1) on the measurements as the measurement must now be accurate within a prescribed time period in order to pass the self-test.

4.2.5.13.6 Element 3)O1

This output (used for the self-test) is covered by the self-test (4.2.5.14.1.1) as any failure will be detected by the change in measured resistance when either the resistor is switched into circuit (reduction in value) or out of circuit (increase in value).

4.2.5.13.7 Element 3)T1

Now that the actual measured value can be verified (4.2.5.14.1.1) the claim increases by 85% as all failure modes for medium coverage are now diagnosed.

4.2.5.14 Measure Isolation Resistance – Architecture 3 Plausibility Cross checks

4.2.5.14.1 Isolation Tester PCCs

4.2.5.14.1.1 PCc_ISOT_RES_ST – Isolation Resistance Self-Test

At a predefined rate the PCc will measure the current resistance value, switch in the test resistance and then measure the new resistance. If the measured value equates to the parallel combination of the isolation resistance prior to the test in parallel with the self-test resistor value, then the test has passed and the measured value remains plausible. A significant aspect of this is that the measurement must be seen to change when the resistance is switched into circuit and out of circuit; it is not only checking the parallel combination of resistance.

4.2.5.15 Measure Isolation Resistance – Architecture 3 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 46 and the LFM calculation shown in Table 47.

Table 46: Measure Isolation Resistance Architecture 3 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical failure rate	Failure rate distribution, %	Safety Critical Failure rate	Failure mode that can violate safety goal w/o safety mechanisms?	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Connections											
HVPOS_AI_1V0	Connection	3)C1	0.0353	y	0.0353	45%	0.0159	y	PCc_Ref_WIN	99.00%	0.0002
HVNEG_AI_1V0	Connection	3)C2	0.0353	y	0.0353	45%	0.0159	y	PCc_Ref_WIN	99.00%	0.0002
Isolation Monitor Inputs											
HVPOS_AI_1V0	Measurement	3)M1	4.9000	y	4.9000	45%	2.2050	y	PCc_Ref_WIN. PCc_ISOT_RES_ST	93.50%	0.1434
HVNEG_AI_1V0	Measurement	3)M2	4.9000	Y	4.9000	45%	2.2050	y	PCc_Ref_WIN. PCc_ISOT_RES_ST	93.50%	0.1434
CHASSIS_AI_1V0	Connection	3)C3	0.0353	Y	0.0353	45%	0.0159	y	PCc_ISOT_RES_ST	72.00%	0.0045
Isolation Monitor Internal								x			
STR_ISOL_HV_1V0 STR_ISOL_RES_DP_1KR0	Transducer	3)T1	14.3674	Y	14.3674	45%	6.4653	y	PCc_REF_WINDOW	84.98%	0.9709
STR_ISOL_HV_1V0	Parameter	1)P1	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97%	0.1197
STR_ISOL_RES_DP_1V0	Parameter	2)P3	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.24%	0.1108
Power Supply	General - PSU	1)PSU1	12.0000	Y	12.0000	45%	5.4000	y	PCc_PSU_MON	98.51%	0.0807
Isolation Monitor Outputs											
TEST_RES_EN	Output	3)O1	3.0000	Y	3.0000	45%	1.3500	y	PCc_EXT_RES_ST	84%	0.2205
Isolation Monitor Outputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D1	3.9991	Y	3.9991	45%	1.7996	y	PCc_REF_WINDOW	95.89%	0.0740
TEST_RES_EN	Actuator	3)A1	15.0000	Y	15.0000	45%	6.7500	y	PCc_EXT_RES_ST	74%	1.7760
String Inputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D4	3.9991	Y	3.9991	45%	1.7996	y	PCc_REF_WINDOW	95.89%	0.0740
String Internal											
STR_ISOL_HV_DP_1V0_TX	Parameter	2)P6	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.02%	0.1197
Power Supply	General - PSU	1)PSU2	12.0000	Y	12.0000	45%	5.4000	y	PCc_PSU_MON	98.51%	0.0807
Total FR (FIT)			**101.037**		**101.037**						**3.919**
										Single Point Fault Metric	**96.1%**

Table 47: Measure Isolation Resistance Architecture 3 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical failure rate	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Element Reference	Failure Mode coverage with respect to Latent failures, %	Latent.multiple-Point failure rate/FIT
Connections											
HVPOS_AI_1V0	Connection	3)C1	0.0353	y	0.0353	0.0157	Y	SC_EXT_REF		90%	0.0016
HVNEG_AI_1V0	Connection	3)C2	0.0353	y	0.0353	0.0157	Y	SC_EXT_REF		90%	0.0016
Isolation Monitor Inputs											
HVPOS_AI_1V0	Measurement	3)M1	4.9000	y	4.9000	2.0616	Y	SC_EXT_REF		90%	0.2062
HVNEG_AI_1V0	Measurement	3)M2	4.9000	Y	4.9000	2.0616	Y	SC_EXT_REF		90%	0.2062
CHASSIS_AI_1V0	Connection	3)C3	0.0353	Y	0.0353	0.0114	Y	SC_EXT_REF		90%	0.0011
Isolation Monitor Internal											
STR_ISOL_HV_1V0 STR_ISOL_RES_DP_1KR0	Transducer	3)T1	14.3674	Y	14.3674	5.4944	Y	SC_EXT_REF		90%	0.5494
STR_ISOL_HV_1V0	Parameter	1)P1	8.9218	Y	8.9218	3.8951	Y	Wdog		60%	1.5580
STR_ISOL_RES_DP_1V0	Parameter	2)P3	8.9218	Y	8.9218	3.9040	Y	Wdog		60%	1.5616
Power Supply	General - PSU	1)PSU1	12.0000	Y	12.0000	5.3193	Y	Wdog		60%	2.1277
Isolation Monitor Outputs											
TEST_RES_EN	Output	3)O1	3.0000	Y	3.0000	1.1295					
Isolation Monitor Outputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D1	3.9991	Y	3.9991	1.7256					
TEST_RES_EN	Actuator	3)A1	15.0000	Y	15.0000	4.9740					
String Inputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D4	3.9991	Y	3.9991	1.7256					
String Internal											
STR_ISOL_HV_DP_1V0_TX	Parameter	2)P6	8.9218	Y	8.9218	3.8951	Y	Wdog		60%	1.5580
Power Supply	General - PSU	1)PSU2	12.0000	Y	12.0000	5.3193	Y	Wdog		60%	2.1277
Total FR (FIT)			**101.037**		**101.037**						**9.899**
									Latent Fault metric		**89.8%**

A significant jump of 11.6% to 96.1% is achieved for the SPFM (Table 46). The LFM has also improved slightly. These values mean that the architecture now satisfies ASIL B for the architectural metric requirements. The architecture is now close to satisfying ASIL C architectural metrics, an improvement of 0.9% is required, and this can be achieved even if the LFM was reduced as this is well within the target area for ASIL C (>80%).

4.2.5.16 Measure Isolation Resistance – Architecture 4

One idea is to move PCc_ISOT_RES_ST to the string controller to give it a level of independence. This offers some advantages:

1) The self-test can now be operated asynchronously to the measurement in the Isolation Tester.

2) The String Controller would know when it was requesting the self-test and would know to expect the drop in measured resistance (if the self-test functioned correctly).
3) It is likely to reduce latent faults (in that there was some independence in the self-test).
4) It offers a route to a level of ASIL decomposition (BSI, 2011).

It does, however, have the disadvantage that to perform Isolation Resistance monitoring two controllers are required. This was not thought a significant disadvantage as isolation monitoring is only required for systems operating at a voltage greater than 60Vdc (UN ECE Reg 100, 2013) and this typically requires and additional controller for the battery management / string control.

The new architecture is shown in Figure 15.

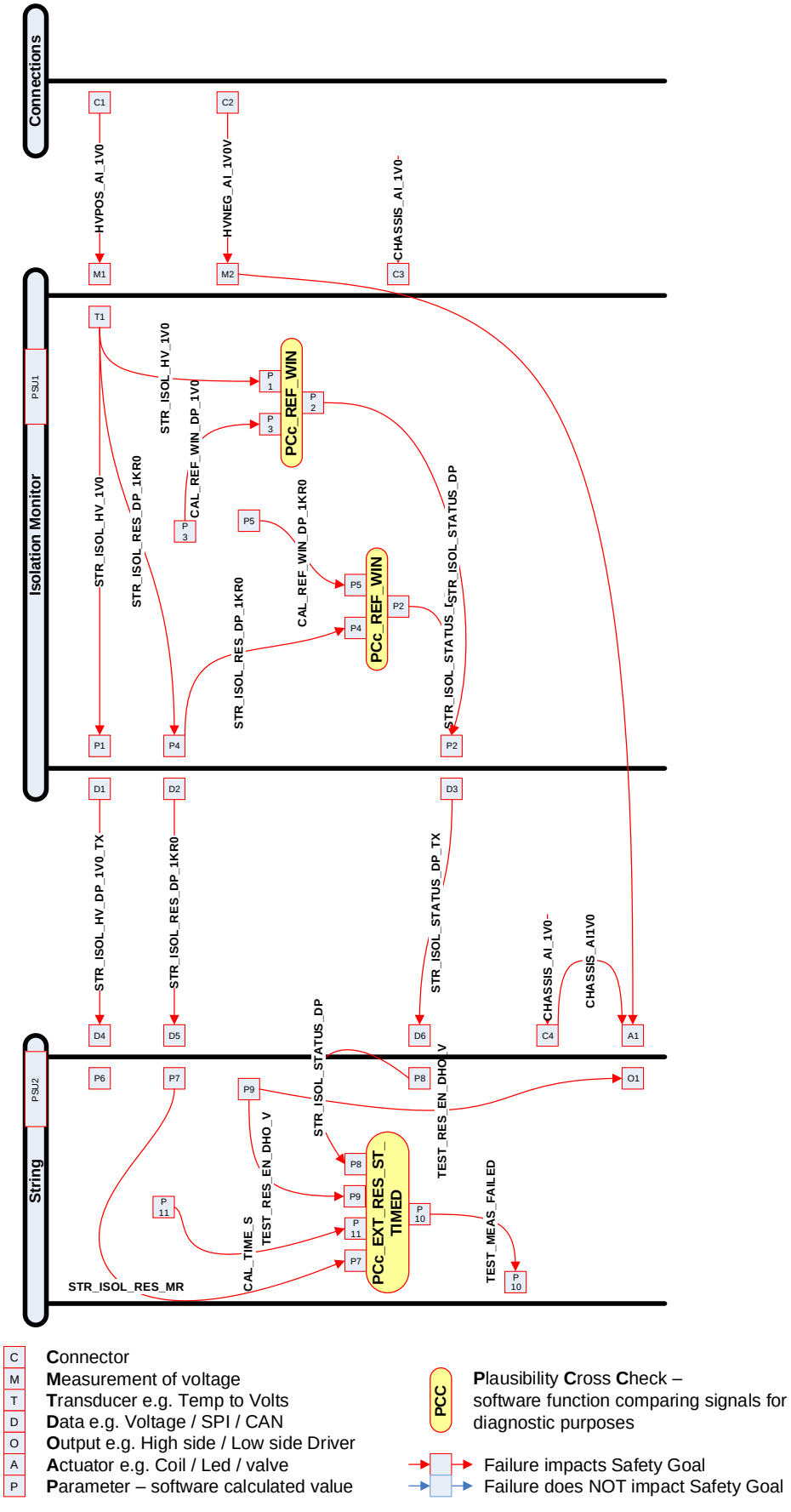


Figure 15: Measure Isolation Resistance – System Diagram - Architecture 4

4.2.5.17 Measure Isolation Resistance – Architecture 4 Classified Signals

To implement the PCc in another controller requires some of the function blocks and connection to move from the Isolation Tester to the String Controller. Generally, the element types and signal names have remained the same and so are not repeated in this section and effectively only one new signal is added (discussed below). The relevant PCcs that are applied are discussed in subsequent sections.

4.2.5.17.1 Isolation Tester Internal Signals

4.2.5.17.1.1 C4 - CHASSIS_AI_1V0

One improvement is to add a separate chassis connection. This has the advantage that it is proving both the chassis connection to the string controller and the chassis connection to the isolation tester, rather than the self-test being performed through another ground route such as the ground connection of the 12V power supply.

4.2.5.17.1.2 P10 - TEST_MEAS_FAILED_DP

To differentiate the self-test failure, TEST_MEAS_FAILED_DP is added rather than using a repeat of the STR_ISOL_STATUS_DP signal as used in the Isolation Tester. This would be set as before when the isolation measurement failed to correctly report the self-test / HV – chassis parallel resistance correctly.

4.2.5.18 Measure Isolation Resistance – Architecture 4 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section4.2.5.19. Table 48 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 48: MIR Architecture 4 Element Cross Reference to Diagnostic Coverage Claims

Element	**Diagnostic Coverage Calculation Table Reference in Appendix D4 – MIR – Architecture 4 DC% Claims**
4)C4	Table 118: MIR – Architecture 4 Connection 4

4.2.5.18.1 Element 4)C4

Moving the self-test (4.2.5.19.1.1) to an external system immediately offers high coverage for this connection as it can be independently verified as being correct.

4.2.5.19 Measure Isolation Resistance – Architecture 4 Plausibility Cross checks

4.2.5.19.1 Isolation Tester PCCs

4.2.5.19.1.1 PCc_EXT_RES_ST– External Isolation Resistance Self-Test

This is identical to PCc_ISOT_RES_ST discussed in 4.2.5.14.1.1, however it is now external to the Isolation Tester.

4.2.5.20 Measure Isolation Resistance – Architecture 4 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 49 and the LFM calculation shown in Table 50.

Table 49: Measure Isolation Resistance Architecture 4 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Safety Critical Failure rate	Failure mode that can violate safety goal w/o safety mechanisms?	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Connections											
HVPOS_AI_1V0	Connection	3)C1	0.0353	y	0.0353	45%	0.0159	y	PCc_Ref_WIN	99%	0.0002
HVNEG_AI_1V0	Connection	3)C2	0.0353	y	0.0353	45%	0.0159	y	PCc_Ref_WIN	99%	0.0002
Isolation Monitor Inputs											
HVPOS_AI_1V0	Measurement	3)M1	4.9000	y	4.9000	45%	2.2050	y	PCc_Ref_WIN. PCc_ISOT_RES_ST	93%	0.1434
HVNEG_AI_1V0	Measurement	3)M2	4.9000	Y	4.9000	45%	2.2050	y	PCc_Ref_WIN. PCc_ISOT_RES_ST	93%	0.1434
CHASSIS_AI_1V0	Connection	3)C3	0.0353	Y	0.0353	45%	0.0159	y	PCc_ISOT_RES_ST	72%	0.0045
Isolation Monitor Internal											
STR_ISOL_HV_1V0 STR_ISOL_RES_DP_1KR0	Transducer	3)T1	14.3674	Y	14.3674	45%	6.4653	y	PCc_REF_WINDOW	85%	0.9709
STR_ISOL_HV_1V0	Parameter	1)P1	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.02%	0.1197
STR_ISOL_RES_DP_1V0	Parameter	2)P3	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.24%	0.1108
Power Supply	General - PSU	1)PSU1	12.0000	Y	12.0000	45%	5.4000	y	PCc_PSU_MON	98.51%	0.0807
Isolation Monitor Outputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D1	3.9991	Y	3.9991	45%	1.7996	y	PCc_REF_WINDOW	95.89%	0.0740
String Inputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D4	3.9991	Y	3.9991	45%	1.7996	y	PCc_REF_WINDOW	95.89%	0.0740
CHASSIS_AI_1V0	Connection	4)C4	0.0353	Y	0.0353	45%	0.0159	y	PCc_EXT_RES_ST	99%	0.0002
String Internal											
STR_ISOL_HV_DP_1V0_TX	Parameter	2)P6	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.02%	0.1197
TEST_RES_EN	Output	3)O1	3.0000	Y	3.0000	45%	1.3500	y	PCc_EXT_RES_ST	84%	0.2205
Power Supply	General - PSU	1)PSU2	12.0000	Y	12.0000	45%	5.4000	y	PCc_PSU_MON	98.51%	0.0807
String Outputs											
TEST_RES_EN	Actuator	3)A1	15.0000	Y	15.0000	45%	6.7500	y	PCc_EXT_RES_ST	74%	1.7760
Total FR (FIT)			**101.072**		**101.072**						**3.919**
									Single Point Fault Metric		**96.1%**

Table 50: Measure Isolation Resistance Architecture 4 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Element refernce	Failure Mode coverage with respect to Latent failures, %	Latent.multiple-Point failure rate/FIT
Connections											
HVPOS_AI_1V0	Connection	3)C1	0.0353	y	0.0353	0.0157	Y	SC_EXT_REF		90%	0.0016
HVNEG_AI_1V0	Connection	3)C2	0.0353	y	0.0353	0.0157	Y	SC_EXT_REF		90%	0.0016
Isolation Monitor Inputs											
HVPOS_AI_1V0	Measurement	3)M1	4.9000	y	4.9000	2.0616	Y	SC_EXT_REF		90%	0.2062
HVNEG_AI_1V0	Measurement	3)M2	4.9000	Y	4.9000	2.0616	Y	SC_EXT_REF		90%	0.2062
CHASSIS_AI_1V0	Connection	3)C3	0.0353	Y	0.0353	0.0114	Y	SC_EXT_REF		90%	0.0011
Isolation Monitor Internal											
STR_ISOL_HV_1V0 STR_ISOL_RES_DP_1KR0	Transducer	3)T1	14.3674	Y	14.3674	5.4944	Y	SC_EXT_REF		90%	0.5494
STR_ISOL_HV_1V0	Parameter	1)P1	8.9218	Y	8.9218	3.8951	Y	Wdog		60%	1.5580
STR_ISOL_RES_DP_1V0	Parameter	2)P3	8.9218	Y	8.9218	3.9040	Y	Wdog		60%	1.5616
Power Supply	General - PSU	1)PSU1	12.0000	Y	12.0000	5.3193	Y	Wdog		60%	2.1277
Isolation Monitor Outputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D1	3.9991	Y	3.9991	1.7256					
String Inputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D4	3.9991	Y	3.9991	1.7256					
CHASSIS_AI_1V0	Connection	4)C4	0.0353	Y	0.0353	0.0157					
String Internal											
STR_ISOL_HV_DP_1V0_TX	Parameter	2)P6	8.9218	Y	8.9218	3.8951	Y	Wdog		60%	1.5580
TEST_RES_EN	Output	3)O1	3.0000	Y	3.0000	1.1295					
Power Supply	General - PSU	1)PSU2	12.0000	Y	12.0000	5.3193	Y	Wdog		60%	2.1277
String Outputs											
TEST_RES_EN	Actuator	3)A1	15.0000	Y	15.0000	4.9740					
Total FR (FIT)			**101.072**		**101.072**						**9.899**
										Latent Fault metric	**89.8%**

This gives no change in the architectural metrics, even though a slight increase was initially expected. As the PCc analysis is using effectively the same lumped models and just moving them between controllers then the only remaining difference is the addition of the chassis connection. The failure rate of this (0.0353 FIT) is very small when compared to the overall safety critical failure rate (101 FIT) which explains why the same metrics were achieved.

One remaining area for possible improvement is to monitor the timing of the self-test function to ensure that it is being run at the correct rate. This is discussed in Architecture 5 (4.2.5.21).

4.2.5.21 Measure Isolation Resistance – Architecture 5

The aim of architecture 5 is to ensure correct operation of the self-test function timing and increase the architectural metrics to achieve ASIL C targets.

The self-test is provided with an additional calibrated time window that is independently monitored to ensure that the isolation resistance dips to the warning level and the internal warning (based on self-test) flag is set within the time window. This effectively proves that the self-test and warning detection functions are all working. The new architecture is shown in Figure 16.

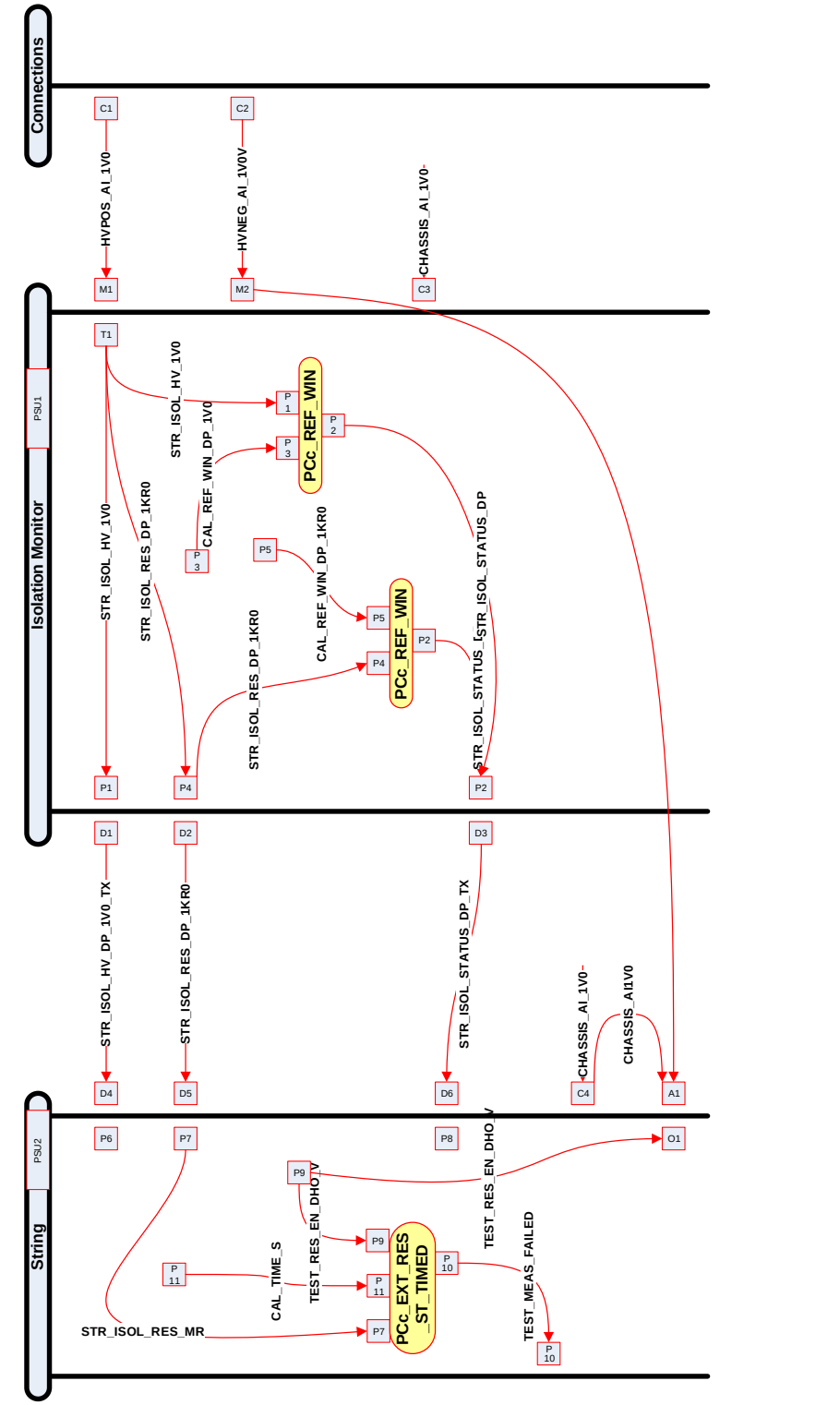


Figure 16: Measure Isolation Resistance – System Diagram - Architecture 5

4.2.5.22 Measure Isolation Resistance – Architecture 5 Classified Signals

4.2.5.22.1 Isolation Tester Internal Signals

4.2.5.22.1.1 P11 – CAL_TIME_S

The calibration time. This is an array of parameters to cover minimum time and maximum time for the self-test. It will also need times from start up as the first isolation measurement time is normally longer.

4.2.5.22.1.2 P10 - TEST_MEAS_FAILED_DP

To differentiate the self-test failure, TEST_MEAS_FAILED_DP is added rather than using a repeat of the STR_ISOL_STATUS_DP signal as used in the Isolation Tester. This would be set as before when the isolation measurement failed to correctly report the self-test / HV – chassis parallel resistance correctly.

4.2.5.23 Measure Isolation Resistance – Architecture 5 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.2.5.24. Table 51 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 51: MIR Architecture 5 Element Cross Reference to Diagnostic Coverage Claims

Element	**Diagnostic Coverage Calculation Table Reference in Appendix D5 – MIR – Architecture 5 DC% Claims**
5)M1	Table 119: MIR – Architecture 5 Measurement 1
5)M2	Refer to 5)M1 as similar techniques used
5)T1	Table 120: MIR – Architecture 5 Transducer 1

4.2.5.23.1 Element 5)M1, 5)M2

An improvement of nearly 4% is achieved by having independent timing on the self-test function (4.2.5.24.1.1).

4.2.5.23.2 Element 5)T1

A 14% increase in coverage is provided due to the independence between the self-test (4.2.5.24.1.1) monitoring functions and their associated timing.

4.2.5.24 Measure Isolation Resistance – Architecture 5 Plausibility Cross checks

4.2.5.24.1 Isolation Tester PCCs

4.2.5.24.1.1 PCc_EXT_RES_ST_TIMED– External Isolation Resistance Self-Test Timed

This is based on PCc_ISOT_RES_ST discussed in 4.2.5.14.1.1, however it now has a method to cross check the timing between the String Controller and the Isolation Tester.

4.2.5.25 Measure Isolation Resistance – Architecture 5 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 52 and the LFM calculation shown in Table 53.

Table 52: Measure Isolation Resistance Architecture 5 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety critical failure rate	Failure rate distribution, %	Safety Critical Failure rate	Failure mode that can violate safety goal w/o safety mechanisms?	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Connections											
HVPOS_AI_1V0	Connection	3)C1	0.0353	y	0.0353	45%	0.0159	y	PCc_Ref_WIN	99.00%	0.0002
HVNEG_AI_1V0	Connection	3)C2	0.0353	y	0.0353	45%	0.0159	y	PCc_Ref_WIN	99.00%	0.0002
Isolation Monitor Inputs											
HVPOS_AI_1V0	Measurement	5)M1	4.9000	y	4.9000	45%	2.2050	y	PCc_Ref_WIN, PCc_EXT_RES_ST_TIMED	97.32%	0.0592
HVNEG_AI_1V0	Measurement	5)M2	4.9000	Y	4.9000	45%	2.2050	y	PCc_Ref_WIN, PCc_EXT_RES_ST_TIMED	97.32%	0.0592
CHASSIS_AI_1V0	Connection	3)C3	0.0353	Y	0.0353	45%	0.0159	y	PCc_ISOT_RES_ST	72.00%	0.0045
Isolation Monitor Internal								x			
STR_ISOL_HV_1V0 STR_ISOL_RES_DP_1KR0	Transducer	5)T1	14.3674	Y	14.3674	45%	6.4653	y	PCc_REF_WIN, Cc_EXT_RES_ST_TIMED	98.33%	0.1079
STR_ISOL_HV_1V0	Parameter	1)P1	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.02%	0.1197
STR_ISOL_RES_DP_1V0	Parameter	2)P3	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.24%	0.1108
Power Supply	General - PSU	1)PSU1	12.0000	Y	12.0000	45%	5.4000	y	PCc_PSU_MON	98.51%	0.0807
Isolation Monitor Outputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D1	3.9991	Y	3.9991	45%	1.7996	y	PCc_REF_WINDOW	95.89%	0.0740
String Inputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D4	3.9991	Y	3.9991	45%	1.7996	y	PCc_REF_WINDOW	95.89%	0.0740
CHASSIS_AI_1V0	Connection	4)C4	0.0353	Y	0.0353	45%	0.0159	y	PCc_EXT_RES_ST	99%	0.0002
String Internal											
STR_ISOL_HV_DP_1V0_TX	Parameter	2)P6	8.9218	Y	8.9218	45%	4.0148	y	PCc_PSU_MON	97.02%	0.1197
TEST_RES_EN	Output	3)O1	3.0000	Y	3.0000	45%	1.3500	y	PCc_EXT_RES_ST	84%	0.2205
Power Supply	General - PSU	1)PSU2	12.0000	Y	12.0000	45%	5.4000	y	PCc_PSU_MON	98.51%	0.0807
String Outputs											
TEST_RES_EN	Actuator	3)A1	15.0000	Y	15.0000	45%	6.7500	y	PCc_EXT_RES_ST	74%	1.7760
Total FR (FIT)			**101.072**		**101.072**						**2.887**
										Single Point Fault Metric	**97.1%**

Table 53: Measure Isolation Resistance Architecture 5 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety critical failure rate	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Element reference	Failure Mode coverage with respect to Latent failures, %	Latent.multiple-Point failure rate/FIT
Connections											
HVPOS_AI_1V0	Connection	3)C1	0.0353	y	0.0353	0.0157	Y	SC_EXT_REF		90%	0.0016
HVNEG_AI_1V0	Connection	3)C2	0.0353	y	0.0353	0.0157	Y	SC_EXT_REF		90%	0.0016
Isolation Monitor Inputs											
HVPOS_AI_1V0	Measurement	5)M1	4.9000	y	4.9000	2.1458	Y	SC_EXT_REF		90%	0.2146
HVNEG_AI_1V0	Measurement	5)M2	4.9000	Y	4.9000	2.1458	Y	SC_EXT_REF		90%	0.2146
CHASSIS_AI_1V0	Connection	3)C3	0.0353	Y	0.0353	0.0114	Y	SC_EXT_REF		90%	0.0011
Isolation Monitor Internal											
STR_ISOL_HV_1V0 STR_ISOL_RES_DP_1KR0	Transducer	5)T1	14.3674	Y	14.3674	6.3575	Y	SC_EXT_REF		90%	0.6357
STR_ISOL_HV_1V0	Parameter	1)P1	8.9218	Y	8.9218	3.8951	Y	Wdog		60%	1.5580
STR_ISOL_RES_DP_1V0	Parameter	2)P3	8.9218	Y	8.9218	3.9040	Y	Wdog		60%	1.5616
Power Supply	General - PSU	1)PSU1	12.0000	Y	12.0000	5.3193	Y	Wdog		60%	2.1277
Isolation Monitor Outputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D1	3.9991	Y	3.9991	1.7256					
String Inputs											
STR_ISOL_HV_DP_1V0_TX	Data	2)D4	3.9991	Y	3.9991	1.7256					
CHASSIS_AI_1V0	Connection	4)C4	0.0353	Y	0.0353	0.0157					
String Internal											
STR_ISOL_HV_DP_1V0_TX	Parameter	2)P6	8.9218	Y	8.9218	3.8951	Y	Wdog		60%	1.5580
TEST_RES_EN	Output	3)O1	3.0000	Y	3.0000	1.1295					
Power Supply	General - PSU	1)PSU2	12.0000	Y	12.0000	5.3193	Y	Wdog		60%	2.1277
String Outputs											
TEST_RES_EN	Actuator	3)A1	15.0000	Y	15.0000	4.9740					
Total FR (FIT)			**101.072**		**101.072**						**10.002**
										Latent Fault metric	**89.8%**

This candidate architecture now achieves ASIL C architectural metric targets. This makes use of ASIL decomposition (BSI, 2011) in that the overall safety goal of measuring and reporting isolation resistance is achieved in two systems. If a target of ASIL C was required from the HARA, then the probable route would be to treat the Isolation Tester as the lower ASIL and put the main safety mechanism (the self-test) in the string controller. It is likely that the string controller having overall responsibility for the Battery Management System would be of a higher ASIL which fits with the rules for decomposition:

ASIL C can be ASIL B(C) and ASIL A(C)

With additional requirements as specified in section 4.4.7 in BS ISO 262626 part 9 (BSI, 2011), one of which is proof of independence which is achieved by this candidate architecture.

4.2.5.26 Comparison against Full Architectural Metrics.

To allow the PCc results to be compared, an Isolation Tester was designed in various stages (to match each proposed architecture) to allow the architectural metrics to be calculated for each candidate architecture. The PCcs were generated in more detail as defined for each of the elements and SPFM and LFM calculated.

A number of architectures have been developed and each has a calculated SPFM and LFM value. To validate the accuracy of the results the only route is to perform the SPFM and LFM calculations on the final Isolation Measurement and Reporting System design. This is where considerable effort was required in the detailed design, gathering of failure rate data and failure mode data and analysing every safety critical failure mode for diagnostic coverage.

The candidate architectures led to the final architecture (Architecture 5) that would be taken through to final design. However, to understand how well the predicted SPFM and LFM metrics matched the final results, a design needed to be completed that matched each of the five architectures. To simplify this process, all the data for the components for Architecture 5 was collected. This involved obtaining failure rate data for approximately 140 components. This was either obtained from the manufacturers directly or else calculated from reliability handbooks such as the Reliability Data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment (BSI, 2004). This also gives a breakdown of failure modes and their associated failure mode percentages.

With all the data available, an equivalent schematic was analysed (as per BS ISO 26262 part 5 (BSI, 2011e)) that provided the required functionality and diagnostics as detailed in each of the candidate architectures. This resulted in the final SPFM and LFM values for each of the candidate architectures 1 to 5.

This required a significant amount of effort and is one of the reasons why the PCc method has been developed.

As the full analysis contains more than 400 component failure modes to be analysed, for brevity only the Architecture 5 calculations are included in the appendices. The full SPFM calculations for Architecture 5 are shown in Appendix D6 – MIR – SPFM Calculation – Architecture 5 and the full LFM calculations are shown in Appendix D7 – MIR –LFM Calculation – Architecture 5.

4.2.6 Results.

The results are detailed below (Table 54). This shows the comparison between the SPFM and LFM values achieved for each candidate architecture using the PCc method against the full SPFM and LFM values calculated as per the standard (BSI, 2011e) for the final design implementation.

Table 54: Measure Isolation Resistance Calculation Comparison

			SPFM	LFM
Architecture 1		**PCC**	79.86%	87.55%
		Full	82.14%	92.33%
		Error	-2.27%	-4.78%
Architecture 2		**PCC**	84.55%	88.23%
		Full	87.51%	89.85%
		Error	-2.96%	-1.62%
Architecture 3		**PCC**	96.12%	89.81%
		Full	96.53%	90.98%
		Error	-0.41%	-1.17%
Architecture 4		**PCC**	96.12%	89.81%
		Full	97.31%	91.64%
		Error	-1.19%	-1.83%
Architecture 5		**PCC**	97.14%	89.81%
		Full	98.86%	91.82%
		Error	-1.72%	-2.01%

As can be seen in each case the PCc results show a slightly lower prediction of the SPFM (maximum error of 2.96%) and LFM (maximum error of 4.78%) architectural metric percentages compared to that achieved by the final design. Apart from architecture 1 the trend is for the SPFM (Figure 17) and LFM (Figure 18) values to stay constant or increase as each architecture is developed which is as expected. The only discrepancy is in architecture 1 where the Full LFM percentage is relatively high (92.33%) compared to the PCc prediction (87.55%) The LFM is of lower importance in this case as the value is already within the range for ASIL C.

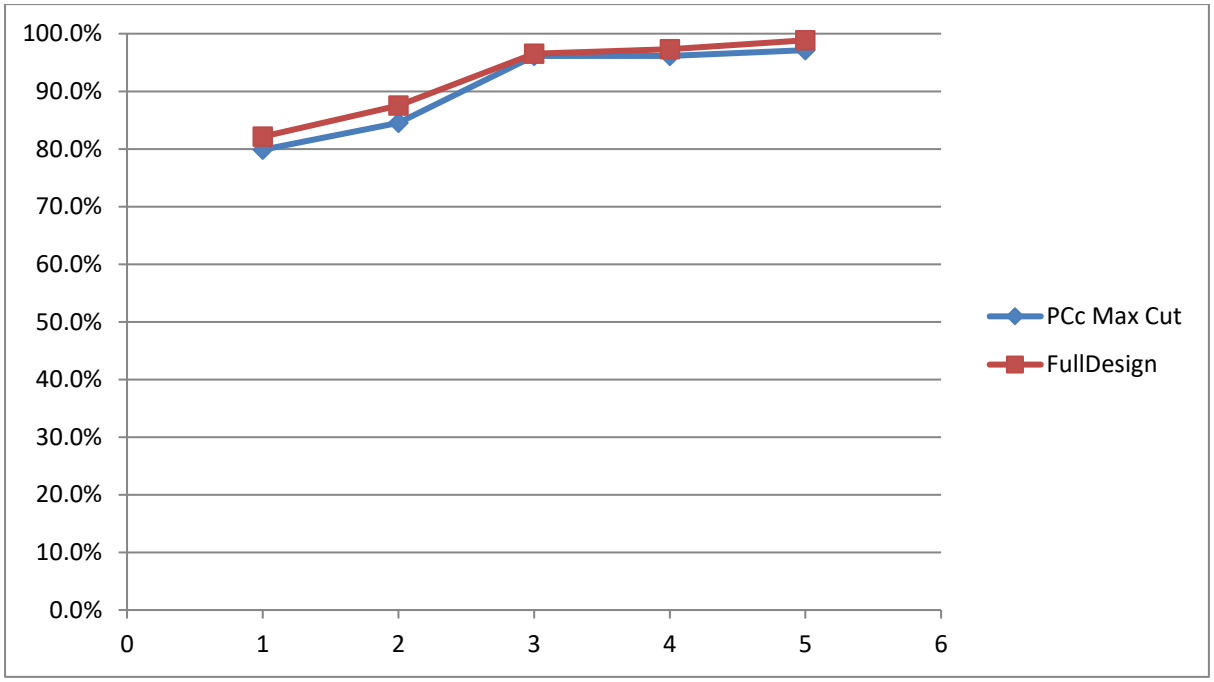


Figure 17: SPFM Comparison for the Measure Isolation Resistance

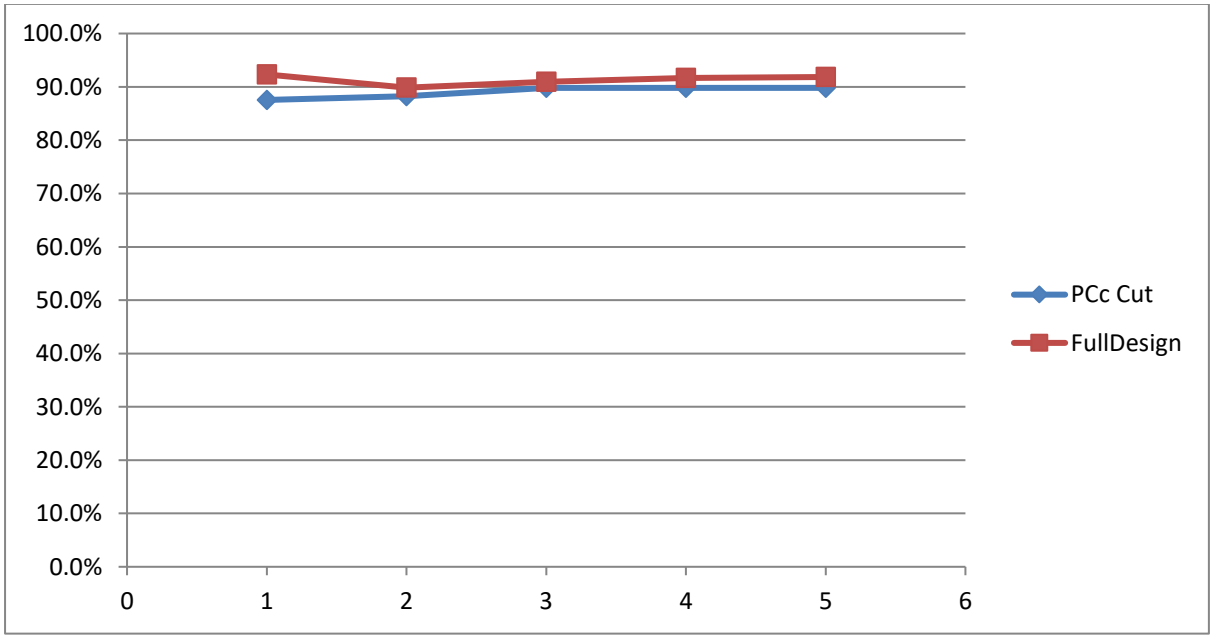


Figure 18: LFM Comparison for the Measure Isolation Resistance

The most important aspect from the results is that, as the architecture is theoretically improved (by the designer adding diagnostic capability or moving diagnostics to provide independence) that the PCc prediction improves allowing a quantified assessment to be made and additional improvements suggested. The results also match that of the Full SPFM calculations i.e. improvements in the PCc calculations are validated by the final design calculations.

The closeness of the results can be explained as follows:

1) The circuits used for the main function (excluding the diagnostics identified throughout the PCc allocation to the candidate architectures) were established and so data was available for the final design. This meant that the lumped models were based on a well-defined selection of components with known failure rates and failure modes.
2) The diagnostic coverage percentages used in the PCc checks were selected from the standards with defined maximum claims and suggested techniques.
3) The techniques selected for the PCc were developed and used in the final design.
4) The final design worked on the diagnostic techniques to the point that they fulfilled the predicted values used in the proposed PCc.
5) The PCc method had defined an architecture that could be implemented in the final design and no significant changes were made between the proposed architecture at the concept level and that completed in the final circuit design. This shows an advantage of the method in that the proposed design can be utilised all the way through to production intent.

The errors between the PCc and full values are considered acceptable and the above results gave the confidence to apply the method to a much more complicated system; the Battery Management System (4.3).

4.3 Battery Management System (BMS)

4.3.1 Hazard Identification and HARA

Prior to conducting the Hazard Analysis and Risk Assessment (HARA) (BSI, 2011c) the hazards applicable to the BMS were identified using a HAZOP – see Appendix B – Hazard Identification. The HARA has not been included in the Thesis as this is a large piece of work covering all the identified hazards considered in all applicable operational situations. The outcome of this work determined an ASIL C classification for overcharge / undercharge of the cells within the battery pack.

4.3.2 Safety Goal Definition

4.3.2.1 Aim - Maintain the cell voltages within their operating area

Manufacturers provide varying levels of detail for their cells. This can take several formats (for example the AMP20M1HD-A cell from A123 Systems (A123 Systems Inc, 2011)) but generally in order to determine a voltage against temperature profile for a cell either the manufacturer has to be contacted through an NDA or else extensive testing has to be performed by the BMS supplier or a nominated third party. This varies with cell chemistry and to a certain extent what manufacturers are prepared to claim to satisfy warranty terms.

The voltage operating area will have an upper and lower limit.

The upper voltage limit would normally be of concern during two use cases:

1) Battery charging when the vehicle is stationary, for example, the on-board or wall mounted (e.g. at home) low power charger or an external high-power charger (e.g. at a service station).
2) Regenerative charging during a drive cycle where energy is recovered when the driver requires the vehicle to slow down during accelerator pedal lift off or braking. This tends to provide a higher current into the cells compared to normal charging, it can also be quite transient in nature due to the nature of the road and driving conditions.

The lower voltage limit is normally of concern during discharge. In this case the vehicle considered only discharge during the drive use case. Additionally, the car can be used as part of the grid system for example to provide power to a house or to the grid system for load balancing.

For the purposes of this example one safety goal has been considered to cover both over and under voltage conditions.

4.3.2.2 Safety Goal

The safety goal is:

> **Ensure the individual cell voltages cannot increase above the maximum operating voltage for a given temperature or decrease below the minimum operating voltage for a given temperature.**

Temperature has specifically been mentioned in the safety goal as the upper and lower voltage curves have a temperature related profile. However, in this analysis, the measured temperature is considered correct so that the analysis concentrates on the voltage measurement only.

It is anticipated that the temperature would be analysed as a separate safety goal with an appropriate ASIL which would independently ensure the safety integrity of the temperature measurement.

The work in this section goes on to develop the system required to satisfy the safety goal using the PCc method. The system is iteratively improved until the architectural metrics meet the required percentages for ASIL C.

4.3.3 System Description

In this example, a different approach has been taken to the Isolation tester (4.2). This demonstrates how the proposed method can be applied to a complete vehicle. This is how a Vehicle OEM may approach the analysis; ultimately, they are responsible for providing a complete safety case for the complete vehicle based on the individual analysis performed for each sub-system (Item as per the BS ISO 26262 definition (BSI, 2011a)).

4.3.4 Sub-system Items

Based on all the sub-system safety goals and known functional requirements a system description diagram can be created. Often, even at the concept stage, the major system components are known and the interfaces between these systems well defined. For example, one of the functions of the BMS is reporting battery operating states and control parameters to external systems. These signal interfaces would have specific requirements for each customer and so not discussed in detail in this Thesis; typical examples would be string / pack current, module / string / pack voltages, module / string / pack temperatures, and control parameters such as maximum discharge current and minimum discharge voltage, maximum regen current and maximum charge current etc.

A similar approach is taken to the other sub-systems and a complete system derived as per the method discussed in3.5.

The author has found this to be an iterative approach and can be used to verify the system diagram against the Item Definition for each sub-system (being considered for functional safety purposes). For reference a basic Item Definition is included in Appendix A – Item Definition. Experience shows that the function descriptions and the interfaces between the functions and external sub-systems lead to a comprehensive but concise item definition.

The overall system can be seen in Figure 19. It is important to show the complete system in terms of functional requirements (not just functional safety requirements). This allows better communication about the system and acts as the initial reference point for interdisciplinary discussion. The aim is to ensure a right first-time approach and this is achieved by availability of common information and a clear understanding of requirements. It also acts as an only source, as the conceptual design progresses (before significant resource is invested in detailed design) all disciples can maintain this diagram with effective communication to all stake holders so that the impact of any system functional requirements can be discussed, reviewed and agreed prior to implementation.

There are several conventions used in battery systems. A suitable convention is discussed by Andrea (Andrea, 2010) who uses the following terms. Additional annotations have been included to aid the system description:

1) Cell – a single cell in a system. Annotated as C'c' where 'c' is the specific cell number.
2) Block – one or more cells connected in parallel to increase the current capacity (i.e. the sum of the individual cell capacities). Annotated as B'b' where 'b' is the specific block number.
3) Battery – a series connection of more than one cell to increase output voltage (i.e. the sum of the series connected cells or blocks). This is often referred to as a module and is annotated as M'm' where 'm' is the specific cell number.
4) String – a series connection of batteries to generate a higher voltage (i.e. the sum of the individual batteries connected in series to form the string). Annotated as S's' where 's' is the specific string number.
5) Pack – a parallel connection of strings to increase the capacity of the pack (i.e. the sum of the parallel connected strings. Annotated as P'p' where 'p' is the specific pack number.

This convention is logical and suits all applications and so has been derived for use in this example.

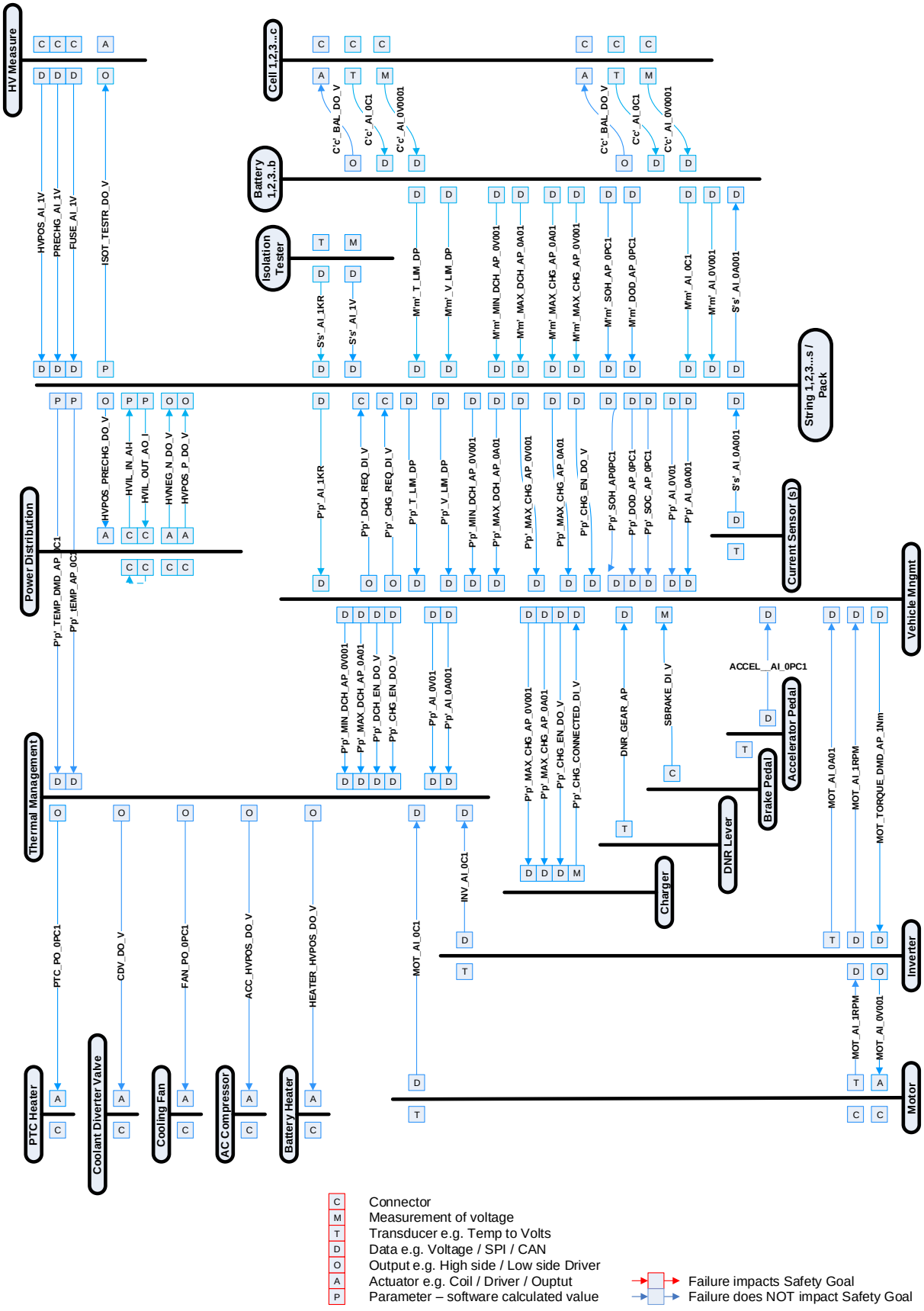


Figure 19: Overall Battery Electric Vehicle System Diagram

4.3.5 System Analysis

The next stage is to define which signals are safety critical for the safety goal under consideration (Figure 20). The critical signals related to the safety goal are highlighted in red in this diagram so that the engineer can see exactly which sub-systems have the capability to violate the safety goal.

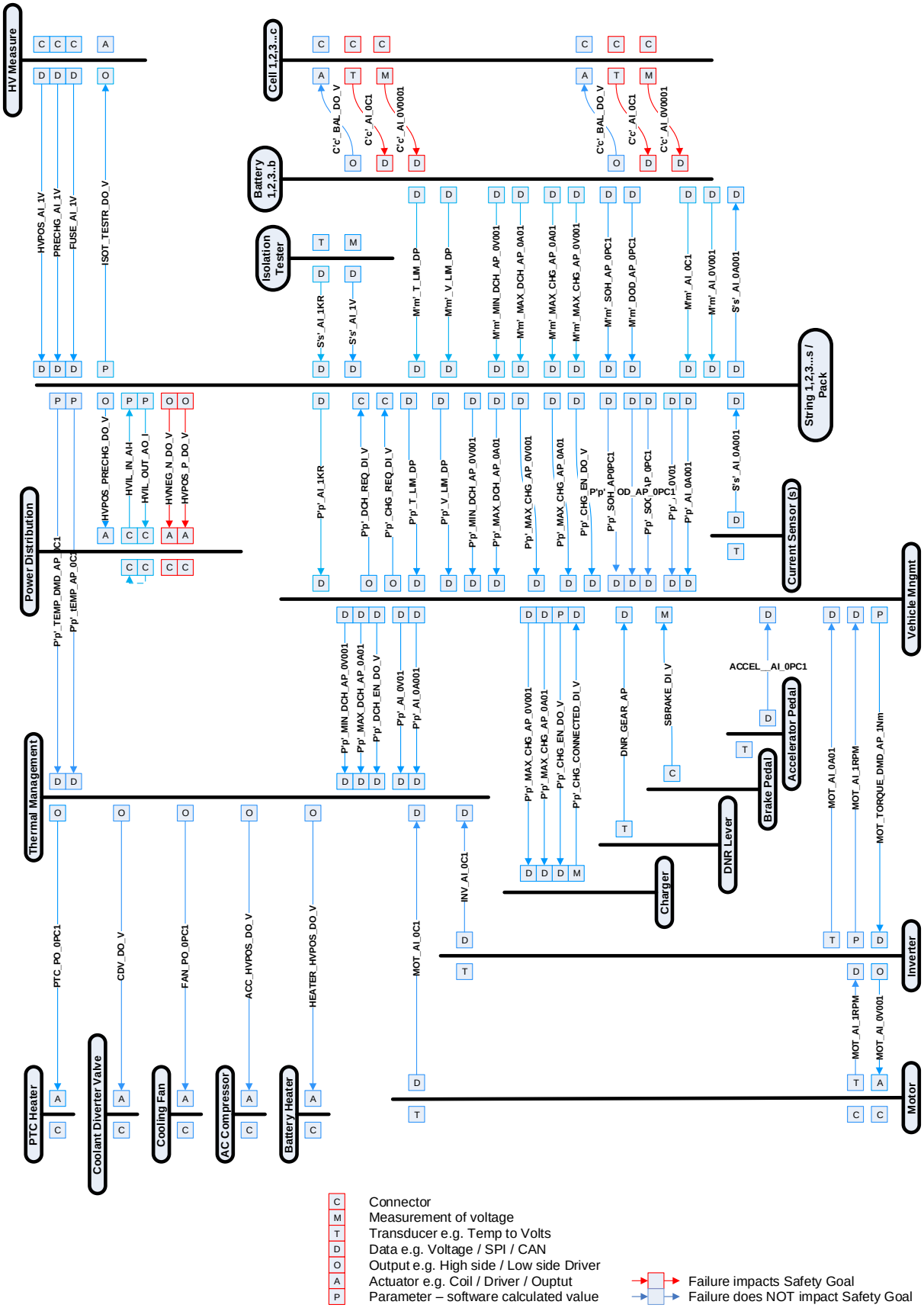


Figure 20: Maintain OA – System Diagram with Safety Critical Signals

4.3.5.1 Conceptual Ideas.

In its most basic form, the system (Figure 21) will have to implement the following functions in order to achieve the safety goal:

1) Measure cell voltages.
2) Measure cell temperatures.
3) Compare the actual cell measurements against a reference table.
4) Prevent further charge or discharge of the cell(s) if the operating limit is exceeded.

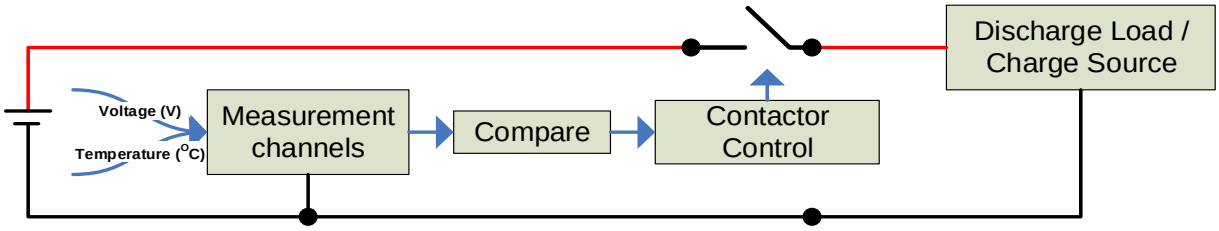


Figure 21: Preliminary Concept

As discussed earlier the cell temperatures are considered correct during the analysis of the cell voltages but the signal is shown as it cannot be ignored when considering violation of the safety goal at the vehicle level.

All faults that can lead to either cell voltages increasing above or decreasing below their pre-defined operating voltage can lead to a violation of the safety goal must be considered when calculating the architectural metrics.

At the concept stage this would be at the signal / interface level such as incorrect measurement i.e. determining a voltage is in range when it is out of range or at the control parameter level such as failure to decide to disconnect the cells from either the load (allowing further discharge) or the source (allowing further charge) when the voltage / temperature calibration profile requires that the cells must be disconnected.

Various possible concept solutions exist which can be hardware based, software based or a combination of the two. Initial assumptions are that a combined system would offer better refinement and therefore an improved driver experience, as software limits can be imposed and the system performance gracefully degraded prior to an absolute disconnect which is likely to be the outcome in a hardware only based solution.

4.3.6 Candidate Selection

As discussed in the proposed method, a candidate architecture is chosen that fulfils the functional requirements and the safety concept without significant emphasis on how the diagnostics will be achieved.

The selection process for this example starts with a relatively simple software control based concept, then examines a different concept (hardware only) and then a combination of the both software control and hardware.

4.3.6.1 Cell Voltage Operating Area – Architecture 1

The architecture measures the cell voltages using an accurate Analogue Front End (AFE). Although the intention of the concept is not to get into specific detail often there are very restricted offerings for devices that meet the functional requirements, accuracy requirements and environmental requirements so in this case a specific device is selected for the concept which is an LTC6803 (Linear Technology, 2011). This has its own self-test functionality (PCc_6803_Self_Test) which is initiated from the battery microcontroller.

The AFE allows voltage measurements (to the required accuracy of +/-5mV) to be compared against pre-determined maximum voltage and minimum voltage limits stored as calibration values in the microcontroller. This is considered a cross check (PCc_OA_Window) as it is used as part of the diagnostic capability to ensure correct cell voltage.

If at any point in time, the PCc_6803_Self_Test or the PCc_OA_Window functions detect a failure in the system this results in the M'm'_TRIP_DP parameter being set which notifies the string microcontroller to open its contactor thus preventing any further increase in voltage due to an external charge source or discharge due to a connected load. As there can be multiple battery modules connected in series to form the string, B'b' is used to indicate battery 1 (_B1_), battery 2 (_B2_) etc.

The architecture places a high degree of responsibility on the software for detecting voltages outside of the limits and shutting down the system.

To perform the analysis more detail is required in terms on internal signals within the sub-system. This highlights an initial problem with the system description diagram (Figure 20) in that the M'm'_TRIP_DP signal is not present between the module microcontroller and the string microcontroller.

The candidate internal architecture, at the item level rather than the vehicle level, is fully developed as shown in Figure 22. It is considered a requirement that there is a route from the module microcontroller to the string microcontroller to trip the system whichever final architecture is adopted and this necessitates an update of the system diagram from that shown in Figure 20 to that shown in Figure 23.

The method now allows us to perform the analysis on this system to determine the types of failure modes that can be detected and the amount of diagnostic coverage that can be achieved. This in turn allows the SPFM and LFM to be calculated for this candidate architecture.

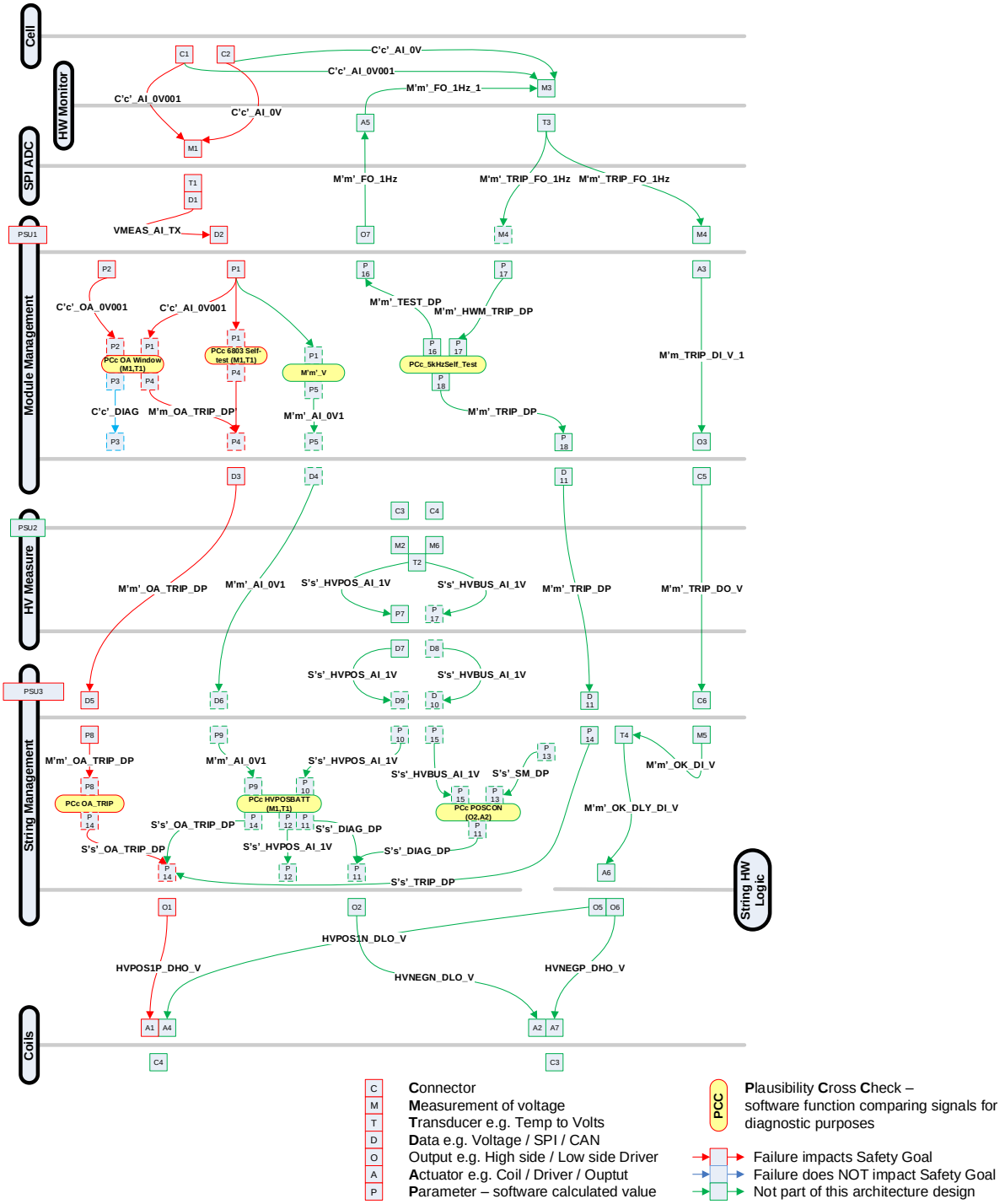


Figure 22: Maintain OA - Concept Architecture Candidate 1

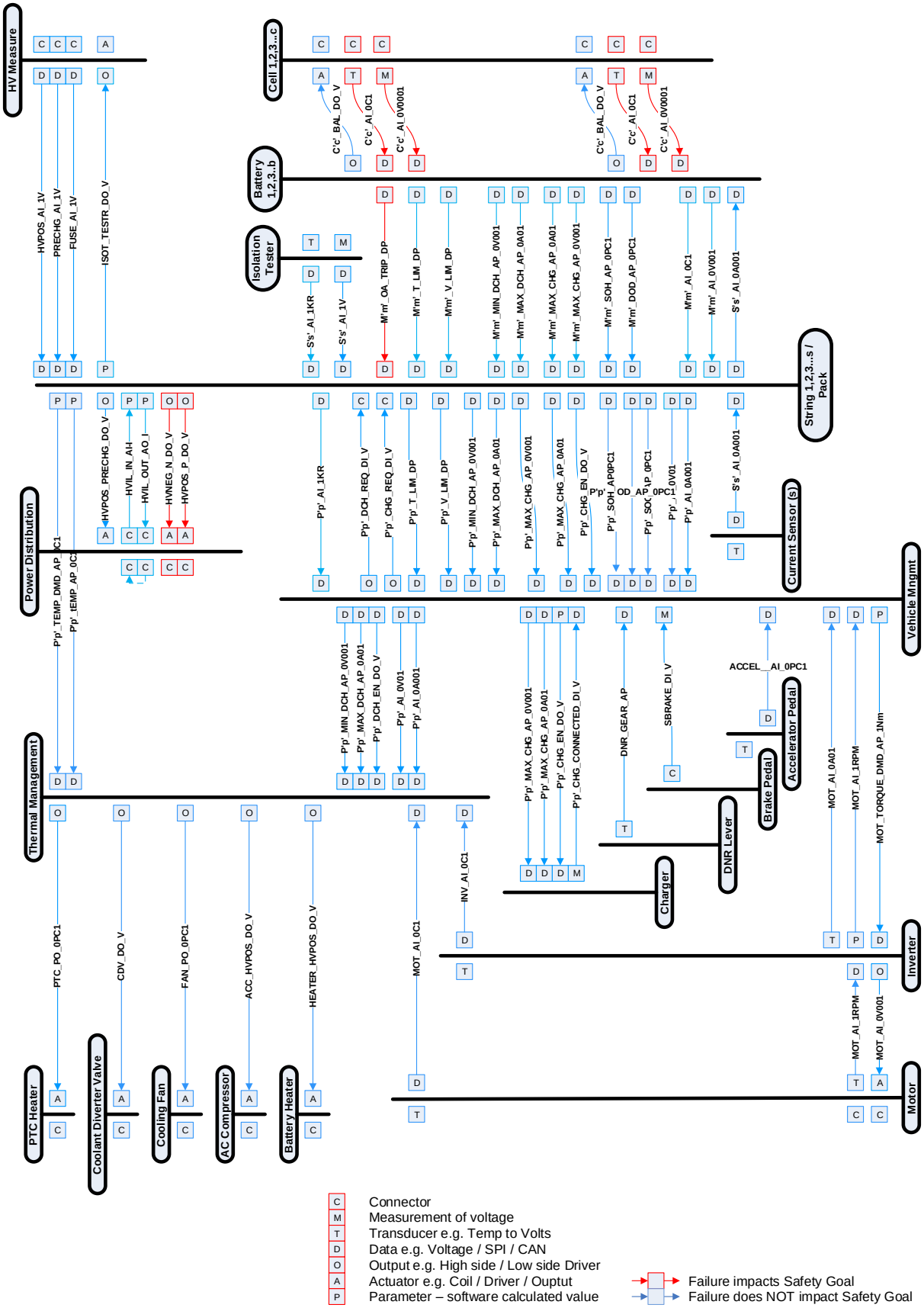


Figure 23: Maintain OA - Safety Critical Signals Update 1

4.3.6.2 Cell Voltage Operating Area - Architecture 1 Classified Signals

To perform the analysis a number of signals are defined which are connected between the critical elements. For clarity, only signals for this candidate architecture diagram (Figure 22) are discussed in this section. The relevant PCcs that are applied are discussed in subsequent sections.

The signals are described as they appear in the architecture diagram (Figure 22) from top left to bottom right.

4.3.6.2.1 Cell

4.3.6.2.1.1 C1 - C'c'_AI_0V001

There is one voltage connection per cell. As the LTC6803 can be configured for many cells (up to a maximum of twelve) the final implementation can vary. For the benefit of this analysis and to assume the maximum failure rate associated with the device, all twelve channels of the LTC6803 are utilised.

This signal is used for the AFE and hardware monitor.

4.3.6.2.1.2 C2 - C'c'_AI_0V

The 0V reference (i.e. is connected to the negative side of cell 'C1').

This signal is used for the AFE and hardware monitor.

4.3.6.2.2 SPI ADC Inputs

4.3.6.2.2.1 M1 - C'c'_AI_0V001

The cell voltage for each cell as received at the AFE for measurement.

4.3.6.2.3 SPI ADC Internal

4.3.6.2.3.1 T1 - VMEAS_AI_TX

The internal logic of the AFE. Although the actual measurement is taken by 'M1' (4.3.6.2.2.1), the AFE is considered sufficiently complicated to be classed as a transducer as it is performing all of the scaling, ADC offset correction and data packaging etc.

4.3.6.2.4 SPI ADC Outputs

4.3.6.2.4.1 D1 - VMEAS_AI_TX

The data transmitted by the AFE. Depending on the request from the cell / battery microcontroller, this data will contain the cell measurements (one per cell) and associated diagnostic information.

4.3.6.2.5 Module Management Inputs

4.3.6.2.5.1 D2 - VMEAS_AI_TX

The data for the measured voltage of each of the cells as received at the module management SPI data input buffer.

4.3.6.2.6 Module Management Internals

4.3.6.2.6.1 PSU1 - Power Supply

The internal power supply for the module microcontroller and any other voltages required by the Module Management system, this would typically be for analogue references etc.

4.3.6.2.6.2 P2 - C'c'_OA_0V001

The internal parameter used as a limit of the cell voltage. As this is an operating window it would contain an upper and lower limit and these would be further modified by temperatures as the safe operating window is temperature dependent.

4.3.6.2.6.3 P1 - C'c'_AI_0V001

The internal parameter for the measure cell voltage. One parameter per cell (i.e. cell 1 to cell 12).

4.3.6.2.6.4 P3 - C'c'_DIAG

The internal parameter is used in the Module Management system to indicate the status of comparison of the cell voltages against the operating area window. It includes status information regarding each individual cell so that the actual cell that trips the module flag M'm'_OA_TRIP_DP (4.3.6.2.6.5) can be typically logged in the data logging system included in Module Management systems.

4.3.6.2.6.5 P4 – M'm'_OA_TRIP_DP

The trip status of the module which indicates that all of the cell voltages C'c'_AI_0V001 are with their operating windows C'c'_OA_0V001 or one or the cells has exceeded either the lower operating area window or the upper operating area window.

4.3.6.2.7 Module Management Outputs

4.3.6.2.7.1 D3 - M'm'_OA_TRIP_DP

The signal M'm'_OA_TRIP_DP (described in 4.3.6.2.6.5) transmitted from the Module Management CAN Bus interface.

4.3.6.2.8 String Management Inputs

4.3.6.2.8.1 D5 - M'm'_OA_TRIP_DP

The signal M'm'_OA_TRIP_DP (see 4.3.6.2.6.5) received at the String Management CAN bus interface.

4.3.6.2.9 String Management Internal

4.3.6.2.9.1 PSU3- Power Supply

The internal power supply for the String Management system. This includes the microcontroller power supply and any other voltages required by the String Management system, this would typically be for analogue references and CAN isolation to the modules (as the modules are not ground referenced to the chassis) whereas the string management logic would be chassis referenced.

4.3.6.2.9.2 P8 – M'm'_OA_TRIP_DP

The internal parameter M'm'_OA_TRIP_DP (see 4.3.6.2.6.5) used by the String Management application.

4.3.6.2.9.3 P9 – M'm'_AI_0V1

The internal parameter M'm'_AI_0V1 used by the String Management application (see equation 18).

$$\boldsymbol{M'm'\_AI\_0V1} = \sum_{'c'=1}^{'c'=12} \boldsymbol{C'c'\_AI\_0V001}$$

Where 'c' is the number of cells and the maximum (12) for the LTC6803 is used in this example.

(18)

4.3.6.2.9.4 P14 – S's'_OA_TRIP_DP

All of the module trips M'M'OA_TRIP_DP (see 4.3.6.2.6.5) are monitored and if any modules trip then the S's'_OA_TRIP_DP parameter is set.

4.3.6.2.10 String Management Outputs

4.3.6.2.10.1 O1 - HVPOS1P_DHO_V

The high side drive of the high voltage positive contactor.

4.3.6.2.11 Coils

4.3.6.2.11.1 A1 - HVPOS1P_DHO_V

The positive side of the high voltage positive contactor coil.

4.3.6.3 Cell Voltage Operating Area - Architecture 1 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.3.6.4. Table 55 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 55: BMS Architecture 1 Element Cross Reference to Diagnostic Coverage Claims

Element	**Diagnostic Coverage Calculation Table Reference in Appendix E1 – BMS – Architecture 1 DC% Claims**
1)A1	Table 121: BMS - Architecture 1 Actuator 1
1)A2	Refer to 1)A1 as similar techniques used
1)C1	Table 122: BMS - Architecture 1 Connection 1
1)C2	Table 123: BMS - Architecture 1 Connection 2
1)C3	Table 124: BMS - Architecture 1 Connection 3
1)C4	Refer to 1)C3 as similar techniques used
1)D1	Table 125: BMS - Architecture 1 Data 1 (subset 1) Table 126: BMS - Architecture 1 Data 1 (subset 2)
1)D2	Refer to 1)D1 as similar techniques used
1)D3	Refer to 1)D1 as similar techniques used
1)D5	Refer to 1)D1 as similar techniques used
1)M1	Table 127: BMS - Architecture 1 Measurement 1
1)M2	Table 128: BMS - Architecture 1 Measurement 2
1)M6	Refer to 1)M2 as similar techniques used
1)O1	Table 129: BMS - Architecture 1 Output 1
1)O2	Table 130: BMS - Architecture 1 Output 2
1)P1	Table 131: BMS - Architecture 1 Parameter 1 (subset 1) Table 132: BMS - Architecture 1 Parameter 1 (subset 2) Table 133: BMS - Architecture 1 Parameter 1 (subset 3)
1)P2	Refer to 1)P1 as similar techniques used
1)P4	Refer to 1)P1 as similar techniques used
1)P5	Refer to 1)P1 as similar techniques used
1)P8	Refer to 1)P1 as similar techniques used

Element	Diagnostic Coverage Calculation Table Reference in Appendix E1 – BMS – Architecture 1 DC% Claims
1)P14	Refer to 1)P1 as similar techniques used
1)PSU1	Table 134: BMS - Architecture 1 Power Supply Unit 1
1)PSU2	Refer to 1)PSU1 as similar techniques used
1)PSU3	Refer to 1)PSU1 as similar techniques used
1)T1	Table 135: BMS - Architecture 1 Transducer 1

4.3.6.3.1 Element '1)A1', 1)A2

Diagnostic coverage is limited to a basic PCC which looks at the power supply (PCc_PSU_Mon 4.2.5.4.4). As there are a number of failure modes not covered that are required for Low diagnostic coverage the PCc claim is reduced to 0.

4.3.6.3.2 Element 1)C1, 1)C2

Initially diagnostics in architecture 1 are limited to the analogue front end internal self-tests - PCc_6803_Self_test (4.3.6.4.2) that can be initiated from the microcontroller.

4.3.6.3.3 Element 1)C3, 1)C4

This is used purely for a diagnostic input in later architectures but they are included here as they have no change in diagnostic coverage through any of the architecture candidates.

4.3.6.3.4 Element 1)D1, 1)D2, 1)D3, 1)D5

PCcs are covered by the standard Data checks (4.2.5.4.1).

4.3.6.3.5 Element 1)M1

Two PCcs are used PCc_6803_Self_Test (4.3.6.4.2) and PCc_OA_Window (4.3.6.4.1) for diagnostic purposes offering low diagnostic coverage.

4.3.6.3.6 Element 1)M2

Measurement 2 is used purely for a diagnostic input in later architectures but is included here as it has no change in diagnostic coverage through any of the architecture candidates.

4.3.6.3.7 Element 1)M6

Measurement 6 is used purely for a diagnostic input in later architectures but is included here as it has no change in diagnostic coverage through any of the architecture candidates.

4.3.6.3.8 Element 1)O1, 1)O2

For the early candidate architectures there are limited diagnostics on the high side driver outputs namely PCc_PSU_Mon (4.2.5.4.4).

4.3.6.3.9 Element 1)P1, 1)P2, 1)P4, 1)P5, 1)P8, 1)P14

Generally, all parameters have similar diagnostics. These vary slightly between those for parameters stored in flash memory and those stored in Random Access memory (RAM). They are covered in detail in 4.2.5.4.3.

4.3.6.3.10 Element 1)PSU1, 1)PSU2, 1)PSU3

The power supplies have the same PCcs - PCc_PSU_Mon (4.2.5.4.4) applied to them.

4.3.6.3.11 Element 1)T1

A number of PCcs are used – PCc_OA_Window (4.3.6.4.1), PCc_6803_Self_Test (4.3.6.4.2) and PCc_PSU_Mon (4.2.5.4.4).

4.3.6.4 Cell Voltage Operating Area - Architecture 1 Plausibility Cross-checks

4.3.6.4.1 PCc_OA_Window

Cells are monitored to be within the specified Operating Area (OA) Window. If individual cell voltages exceed the OA window (defined as an upper and lower voltage limit for a given temperature) for a calibrated time then the software will attempt to reduce current into / out of the system via a maximum set point signal back to the vehicle controller to prevent continued charge or discharge. If this set point demand is not obeyed, the software will normally allow operation to a wider operating window (with a warning to the driver) before ultimately opening the contactors within a specified time. This will prevent the vehicle from being charged or discharged until a suitable reset is actioned. This may be an ignition cycle which then forces a limp home mode or in extreme circumstances a service technician may be required to perform a restart of the vehicle in a tightly controlled environment.

4.3.6.4.2 PCc_6803_Self_Test

The linear device (Linear Technology, 2011) used as the AFE can perform a number of self-tests. These are not performed automatically; rather they are triggered by individual test requests by the microcontroller over the Serial Peripheral Interface (SPI) communications port which connects the microcontroller to the AFE. The integrity of the diagnostic coverage is determined by the number and type of tests performed and their repetition rate. Generally, the software / hardware engineer would decide on the test requirements and determine a method to interleave the tests between the normal cell measurement commands. This is one case where the PCc is determined by a specific device and cannot be generalised. The tests are selected to cover the techniques required by BS ISO 26262 and given the generic classification PCc_6803_Self_Test.

This is considered acceptable in the approach, as the functional requirements will normally dictate a route which in turn limits the choice of device. If several devices are available that can fulfil the functional requirements then many different candidate architectures can be generated using each device in turn which uses representative diagnostic coverage values for each individual device.

In fact, this is another demonstration of where the method allows the architecture to be evaluated early in the project. It may lead directly to a decision as to which analogue front end is to be used in the design based on the architectural metrics demonstrated at the concept stage.

4.3.6.5 Cell Voltage Operating Area – Architecture 1 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 56 and the LFM calculation shown in Table 57.

Table 56: Maintain OA Architecture 1 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Failure mode that has the potential to violate the SG in the absense of a Safety Mechanism	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Cell Connections										
C'c'_AI_0V001	Connection	1)C1	0.6	Y	0.6	45%	Y	PCC 6803 Self test	42.00%	0.1566
C'c'_AI_0V	Connection	1)C2	0.05	Y	0.05	45%	Y	PCC 6803 Self test	72.00%	0.0063
HW Monitor										
C'c'_AI_0V001	Measurement	2)M3	24		0	45%		PCc6801_Self_-Test		
C'c'_AI_0V001	Transducer	2)T3	25		0	45%		6801 Internal functionality, Don't claim 5kHz as not independently proved to be periodic, PCc_PSU_Mon		
SPI ADC Inputs										
C'c'_AI_0V001	Measurement	1)M1	102	Y	102	45%	Y	OA Window, PCC 6803 Self Test	58.80%	18.9108
SPI ADC Internal										
VMEAS_AI_TX	Transducer	1)T1	50	Y	50	45%	Y	6803 Self Test, OA Window	97.74%	0.50900625
SPI ADC Outputs										
VMEAS_AI_TX	Data	1)D1	3	Y	3	45%	Y	PCc_Data_Checksum, Individual poll and response timing	90.79%	0.124308
Module Management Inputs										
VMEAS_AI_TX	Data	1)D2	3	Y	3	45%	Y	PCc_Data_Checksum, Individual poll and response timing	90.79%	0.124308
Module Management Internals										
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	45%	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test	94.08%	0.119930625
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	45%	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test, CRC on CAL Tables	94.37%	0.113972063
Power Supply	General - PSU	1)PSU1	48	Y	48	45%	Y	PCc_PSU_Mon	98.51%	0.32292
Module Management Outputs										
M'm'_OA_TRIP_DP	Data	1)D3	6	Y	6	45%	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.10719
M'm'_TRIP_DP	Data	4)D11	3		0	45%				
HV Measurement Inputs										
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	45%				
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	45%				
HV Measurement Internal										
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	45%				
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%				
S's'_HVPOS_AI_1V	Transducer	1)T2	14		0	45%				
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	45%				
Power Supply	General - PSU	1)PSU2	20		0	45%				
HV Measurement Outputs										
S's'_HVPOS_AI_1V	Data	1)D7	3		0	45%				
String Management Inputs										
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	45%	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.10719
M'm'_TRIP_DP	Data	4)D11	3		0	45%				
String Management Internal										
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	45%	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test	94.08%	0.23986125
Power Supply	General - PSU	1)PSU3	40	Y	40	45%	Y	PCc_PSU_Mon	98.51%	0.2691
String Management Outputs										
HVPOS1P_DHO_V	Output	1)O1	20	Y	20	45%	Y	PCc_PSU_Mon	0.00%	9
HVNEGN_DLO_V	Output	1)O2	20		0	45%				
String Hardware Logic Inputs										
M'm'_OK_DLY_DI_V	Actuator	2)A6	15		0	45%		Refer to element reference	0.00%	
String Hardware Logic outputs										
HVPOS1N_DLO_V	Output		20		0	45%		PCc_PSU_Mon		
HVNEGP_DHO_V	Output		20		0	45%		PCc_PSU_Mon		
Coils										
HVPOS1P_DHO_V	Actuator	1)A1	30	Y	30	100%	Y	PCc_PSU_Mon	0.00%	30
HVNEGN_DLO_V	Actuator	1)A2	30		0	100%				
			542.55		**326.65**		**SPFM =**	**81.6%**		**60.11**

Table 57: Maintain OA Architecture 1 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %		Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Failure Mode coverage with respect to Latent failures, %	Latent:multiple-Point failure rate/FIT
Cell Connections													
C'c'_AI_0V001	Connection	1)C1	0.6	Y	0.6	45%	0.1134	Y	100.00%	0.1134			0.1134
C'c'_AI_0V	Connection	1)C2	0.05	Y	0.05	45%	0.0162	Y	100.00%	0.0162			0.0162
HW Monitor													
C'c'_AI_0V001	Measurement	2)M3	24		0	45%	0			0.0000			
C'c'_AI_0V001	Transducer	2)T3	25		0	45%	0			0.0000			
SPI ADC Inputs													
C'c'_AI_0V001	Measurement	1)M1	102	Y	102	45%	26.9892	Y	100.00%	26.9892			26.9892
SPI ADC Internal													
VMEAS_AI_TX	Transducer	1)T1	50	Y	50	45%	21.99099375	Y	100.00%	21.9910			21.990994
SPI ADC Outputs													
VMEAS_AI_TX	Data	1)D1	3	Y	3	45%	1.225692	Y	100.00%	1.2257			1.225692
Module Management Inputs													
VMEAS_AI_TX	Data	1)D2	3	Y	3	45%	1.225692	Y	100.00%	1.2257			1.225692
Module Management Internals													
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	45%	1.905069375	Y	100.00%	1.9051	Wdog	90.00%	0.1905069
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	45%	1.911027938	Y	100.00%	1.9110	Wdog	90.00%	0.1911028
Power Supply	General - PSU	1)PSU1	48	Y	48	45%	21.27708	Y	100.00%	21.2771	Wdog	90.00%	2.127708
Module Management Outputs													
M'm'_OA_TRIP_DP	Data	1)D3	6	Y	6	45%	2.59281			0.0000			
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
HV Measurement Inputs													
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	45%	0			0.0000			
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	45%	0			0.0000			
HV Measurement Internal													
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	45%	0			0.0000			
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0			0.0000			
S's'_HVPOS_AI_1V	Transducer	1)T2	14		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	45%	0			0.0000			
Power Supply	General - PSU	1)PSU2	20		0	45%	0			0.0000			
HV Measurement Outputs													
S's'_HVPOS_AI_1V	Data	1)D7	3		0	45%	0			0.0000			
String Management Inputs													
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	45%	2.59281	Y	100.00%	2.5928			2.59281
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
String Management Internal													
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	45%	3.81013875	Y	100.00%	3.8101	Wdog	90.00%	0.3810139
Power Supply	General - PSU	1)PSU3	40	Y	40	45%	17.7309	Y	100.00%	17.7309			17.7309
String Management Outputs													
HVPOS1P_DHO_V	Output	1)O1	20	Y	20	45%	0	Y	100.00%	0.0000			0
HVNEGN_DLO_V	Output	1)O2	20		0	45%	0			0.0000			
String Hardware Logic Inputs													
M'm'_OK_DLY_DI_V	Actuator	2)A6	15		0	45%	0			0.0000			
String Hardware Logic outputs													
HVPOS1N_DLO_V	Output		20		0	45%	0			0.0000			
HVNEGP_DHO_V	Output		20		0	45%	0			0.0000			
Coils													
HVPOS1P_DHO_V	Actuator	1)A1	30	Y	30	100%	0	Y	100.00%	0.0000			0
HVNEGN_DLO_V	Actuator	1)A2	30		0	100%	0			0.0000			
			542.55		**326.65**		**LFM =**	**71.9%**					**74.78**

From the above two tables the architecture gives an SPFM of 81.6% (Table 56) and LFM of 71.9% (Table 57). This would only be acceptable in an application with a QM rating for the safety goal and so needs improvement. This was to be expected because the design was based on a functional implementation rather than one specifically aimed at achieving functional safety. This highlights an additional benefit of the proposed method. Before consideration is given to functional safety i.e. when exploring a function, maybe at the proof of concept stage, it is possible to perform a relatively

simple analysis that looks at the base diagnostic capability of the system in a quantified way. This can well influence the architecture long before thoughtful consideration is given to functional safety aspects of the project.

4.3.6.6 Cell Voltage Operating Area – Architecture 2

This second candidate architecture (Figure 24) moves responsibility for maintaining the cells within the operating area from the analogue front-end communication with the microcontroller (software-based solution) to a hardware only solution.

This is achieved by utilising a hardware shutoff mechanism. This approach has the disadvantage that the measurements are not communicated to the battery microcontroller and so the vehicle driver would not be warned about battery state or an impending limp home mode; the battery would just disconnect resulting in loss of drive.

This approach effectively violates other driveline related safety goals in that the driver should be warned if a limp home mode is to be activated (not part of this analysis but a common safety goal generally applied in automotive applications). This architecture is relevant and as such has been analysed in its own right for understanding of what can be achieved with the stand-alone hardware monitor. The basis of this is then used in subsequent architectures which contain both the hardware shut off mechanism and the accurate AFE as discussed in 4.3.6.1.

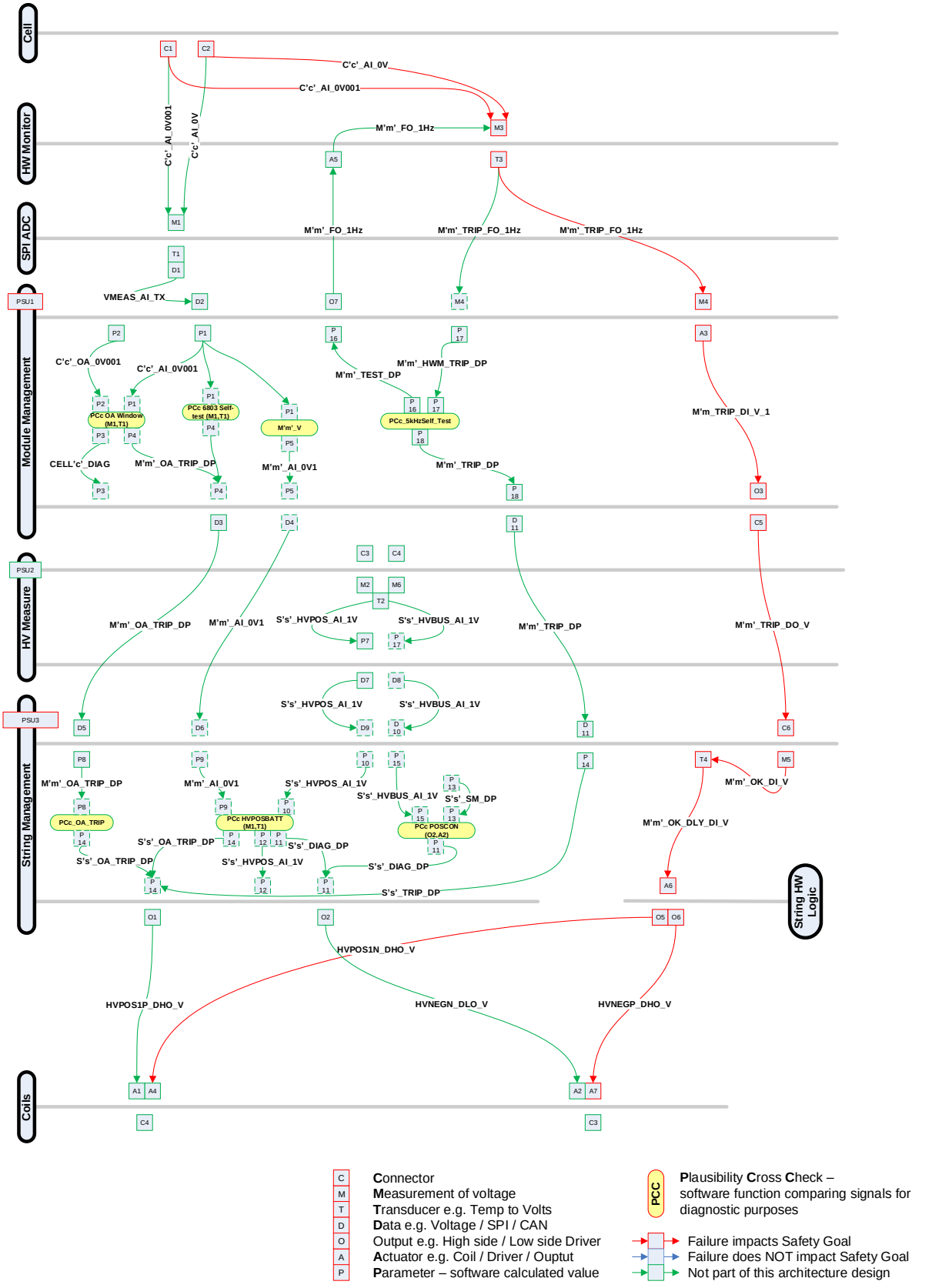


Figure 24: Maintain OA - Concept Architecture Candidate 2

4.3.6.7 Cell Voltage Operating Area – Architecture 2 Classified Signals

All of the signals used in Architecture Candidate 1 (Figure 23) that have been discussed previously in (4.3.6.2) are not duplicated in this section.

4.3.6.7.1 HW Monitor

4.3.6.7.1.1 M3 – C'c'_AI_0V001

The hardware monitor uses the clock input M'm'_FO_1Hz_1 to perform the measurements on the individual cell voltages C'c'_AI_0V001 (4.3.6.2.1.1) in the module.

4.3.6.7.1.2 A5 – M'm'_FO_1Hz_1

The hardware monitor uses the M'm'_FO_1Hz_1 signal as a clock input to the hardware monitor (LTC6801).

4.3.6.7.1.3 T3 – M'm'_TRIP_FO_1Hz

The hardware monitor uses the clock input M'm'_FO_1Hz_1 to run comparative tests between the cell voltages C'c'_AI_0V001 (4.3.6.2.1.1) and the internal upper and lower voltage limits. These limits are configured by input pin configurations that select predefined voltage limits.

4.3.6.7.2 Module Management Inputs

4.3.6.7.2.1 M4 – M'm'_TRIP_FO_1Hz

The measurement of the trip signal based on the hardware monitor transducer output. A frequency signal which is maintained at 5kHz when the LTC6801 is within range.

4.3.6.7.3 Module Management Internals

4.3.6.7.3.1 A3 – M'm'_TRIP_DI_V_1

The frequency input monitored by a window comparator to determine whether the frequency output from the hardware monitor is within appropriate thresholds and then converted to a bi-state voltage which is later used by the String Management system. It is classed as an actuator because it is utilising optical isolation as the measurement side of the module has a different 0V reference to the String Management system.

4.3.6.7.3.2 O3 – M'm'_TRIP_DI_V_1

A voltage output that is later hardwired to the String Management system.

4.3.6.7.4 Module Management Outputs

4.3.6.7.4.1 C5 - M'm'_TRIP_DI_V_1

The hard-wired output from the module management that indicates to the string management that the hardware monitor has tripped.

4.3.6.7.5 String Management Inputs

4.3.6.7.5.1 C6 - M'm'_TRIP_DO_V

M'm'_TRIP_DO_V received as a hardwired signal at the String Management digital input interface.

4.3.6.7.6 String Management Internal

4.3.6.7.6.1 T4 – M'm_OK_DLY_DI_V

M'm'_OK_DLY_DI_V is a time delayed signal. It is time delayed to allowed diagnostics to be performed (the hardware monitor self-test) and monitored (M'm'_OK_DI_V) without it actually tripping the contactors.

4.3.6.7.6.2 M5 – M'm_OK_DI_V

M'm'_OK_DI_V allows the trip voltage to be measured and used by the string management to monitor the status of the hardware monitor both in terms of its actual status and also during and self-tests that are performed.

4.3.6.7.6.3 P14 – S's'_OA_TRIP_DP

All of the module trips M'M'OA_TRIP_DP (see 4.3.6.2.6.5) are monitored and if any modules trip then the S's'_OA_TRIP_DP parameter is set.

4.3.6.7.6.4 P12 – S's'_HVPOS_AI_1V

An internal value used in the String Management system. This is also likely to be transmitted onto the CAN bus for diagnostic purposes and is not considered further as part of the safety critical analysis.

4.3.6.7.6.5 P11 – S's'_DIAG_DP

If the plausibility checks PCc_HVPOSBATT and PCc_POSCoN (see 4.3.6.29 and 4.3.6.34 respectively) detect failures then the S's'_Diag_DP flag is set which can provide a redundant path to open the contactors via O2 – HVPOS1N_DLO_V.

4.3.6.7.7 String Hardware Logic Inputs

4.3.6.7.7.1 A6 - M'm'_OK_DLY_DI_V

The hardware monitored delayed voltage signal (M'm_OK_DLY_DI_V) is converted to an output via actuator A6 which can turn off both the positive and negative contactors via an independent route to the software control outputs.

4.3.6.7.8 String Hardware Logic outputs

4.3.6.7.8.1 O5 – HVPOS1N_DLO_V

The low side drive of the high voltage positive contactor.

4.3.6.7.8.2 O6 – HVNEGP_DHO_V

The high side drive of the high voltage negative contactor.

4.3.6.7.9 Coils

4.3.6.7.9.1 A4 - HVPOS1N_DLO_V

The negative side of the high voltage positive contactor coil.

4.3.6.7.9.2 A7 - HVNEGP_DHO_V

The positive side of the high voltage negative contactor coil.

4.3.6.8 Cell Voltage Operating Area – Architecture 2 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.3.6.9. Table 58 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 58: BMS Architecture 2 Element Cross Reference to Diagnostic Coverage Claims

Element	Diagnostic Coverage Calculation Table Reference in Appendix E2 – BMS – Architecture 2 DC% Claims
2)A3	Table 136: BMS - Architecture 2 Actuator 3
2)A4	Table 137: BMS - Architecture 2 Actuator 4
2)A6	Refer to 2)A4 as similar techniques used
2)A7	Refer to 2)A4 as similar techniques used
2)C1	Table 138: BMS - Architecture 2 Connection 1
2)C2	Refer to 2)C1 as similar techniques used
2)C5	Table 139: BMS - Architecture 2 Connection 5

Element	Diagnostic Coverage Calculation Table Reference in Appendix E2 – BMS – Architecture 2 DC% Claims
2)C6	Refer to 2)C5 as similar techniques used
2)M1	Table 140: BMS - Architecture 2 Measurement 1
2)M3	Table 141: BMS - Architecture 2 Measurement 3
2)M4	Table 142: BMS - Architecture 2 Measurement 4
2)M5	Refer to 2)M4 as similar techniques used
2)O3	Table 143: BMS - Architecture 2 Output 3
2)O5	Table 144: BMS - Architecture 2 Output 5
2)O6	Refer to 2)O5 as similar techniques used
2)T3	Table 145: BMS - Architecture 2 Transducer 3
2)T4	Table 146: BMS - Architecture 2 Transducer 4

4.3.6.8.1 Element '2)A3'

Two PCcs are relied upon the PCc_5kHzSelf_Test (4.3.6.9.2) and the PCc_PSU_Mon (4.2.5.4.4).

4.3.6.8.2 Element '2)A4', 2)A6, 2)A7

PCc_PSU_Mon (4.2.5.4.4) is used for these actuators.

4.3.6.8.3 Element '2)C1', '2C2'

PCc6801_Self_Test is used for these input connections.

4.3.6.8.4 Element '2)C5', 2)C6

In this architecture no diagnostics are used on these connections.

4.3.6.8.5 Element '2)M1'

This uses exactly the same PCcs as in architecture 1 but with additional redundancy built into the system as the AFE is used for control and monitoring and can still trip the system but the safety is purely derived by the LTC 6801 hardware monitoring system. This increases the PCc claim significantly (now 98.21% compared to 58.8% in architecture 1).

4.3.6.8.6 Element '2)M3'

This is a new element in architecture 2 and introduces a new PCc_HW_MONITOR (4.3.6.9.1).

4.3.6.8.7 Element '2)M4'

This is a new element in architecture 2 but no coverage is provided for this element.

4.3.6.8.8 Element '2)M5'

No diagnostics are possible on this measurement.

4.3.6.8.9 Element '2)O3'

The output can be partially verified by the power supply monitoring i.e. if the power supply is correct the output is capable of being driven and to a limited amount the OA trip in software can also be used as a cross check against the intelligent output driver. Diagnostics include PCc_OA_Window (4.3.6.4.1) and PCc_PSU_MON (4.2.5.4.4).

4.3.6.8.10 Element '2)O5', 2)O6

These outputs are not monitored; however, the high side driver power supply is monitored by PCc_PSU_MON (4.2.5.4.4) to prove that the high side drive power is correct.

4.3.6.8.11 Element '2)T3'

The hardware monitor (LTC6801) has a number of internal diagnostics that verify internal operation as detailed in the data sheet (Linear Technology, 2010) which are diagnosed by the PCc6801_Self_Test (4.3.6.9.3).

4.3.6.8.12 Element '2)T4'

The time delay transducer has no verifiable PCc other than proving that the power supply to the time delay block is correct (PCc_PSU_MON (4.2.5.4.4)).

4.3.6.9 Cell Voltage Operating Area – Architecture 2 Plausibility Cross-checks

4.3.6.9.1 PCc_HW_MONITOR

The LTC 6801 acts as a complete hardware monitor and is independent to the microcontroller based system. It has the benefit of being configured in hardware for voltage limits etc. As this acts as a safety mechanism, the configuration links would have to be tested in production to ensure they were correctly set. This may be an optical inspection initially but most likely require an in-circuit test or end of line functional test to prove the safety mechanism operation.

4.3.6.9.2 PCc_5kHzSelf_Test

The 5 kHz self-test is a closed loop test in the Module Management system. The microcontroller is the source of the 5kHz signal. This is only generated as long as the microcontroller is functioning correctly and the software sequencing and timing is correct. The 5kHz signal then drives the internal logic in the LTC6801. The PCc_5kHzSelf_Test ensures that the output is valid only when the input is valid.

4.3.6.9.3 PCc6801_Self_Test

The LTC6801 monitors the cell voltages and temperatures to ensure that they are within range and all the internal self-tests are performed. These are driven by the 5kHz clock signal from the microcontroller.

4.3.6.10 Cell Voltage Operating Area – Architecture 2 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 59 and the LFM calculation shown in Table 60.

Table 59: Maintain OA Architecture 2 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %		Failure mode that has the potential to violate the SG in the absense of a Safety Mechanism	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Connections											
C'c'_AI_0V001	Connection	2)C1	0.6	Y	0.6	45%	0.2700	Y	PCc6801_Self_Test	72.00%	0.0756
C'c'_AI_0V	Connection	2)C2	0.05	Y	0.05	45%	0.0225	Y	PCc6801_Self_Test	72.00%	0.0063
HW Monitor											
C'c'_AI_0V001	Measurement	2)M3	24	Y	24	45%	10.8000	Y	PCc6801_Self_-Test	64.83%	3.79836
C'c'_AI_0V001	Transducer	2)T3	25	Y	25	45%	11.2500	Y	6801 Internal functionality, Don't claim 5kHz as not independently proved to be periodic, PCc_PSU_Mon	72.70%	3.071615625
SPI ADC Inputs											
C'c'_AI_0V001	Measurement	2)M1	102		0	45%	0.0000				
SPI ADC Internal											
VMEAS_AI_TX	Transducer	1)T1	50		0	45%	0.0000				
SPI ADC Outputs											
VMEAS_AI_TX	Data	1)D1	3		0	45%	0.0000				
Module Management Inputs											
VMEAS_AI_TX	Data	1)D2	3		0	45%	0.0000				
M'm'_TRIP_FO_1Hz	Measurement	2)M4	3.5	Y	3.5	45%	1.5750			0.00%	0
Module Management Internals											
C'c'_AI_0V001	Parameter	1)P1	4.5		0	45%	0.0000				
C'c'_OA_0V001	Parameter	1)P2	4.5		0	45%	0.0000				
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	45%	0.4500	Y	PCc_PSU_Mon	98.28%	0.00774
M'm'_TRIP_DI_V	Output	2)O3	25	Y	25	45%	11.2500	Y	PCc_PSU_Mon	59.16%	4.5945
Power Supply	General - PSU	1)PSU1	20	Y	20	45%	9.0000	Y	PCc_PSU_Mon	98.51%	0.13455
Module Management Outputs											
M'm'_TRIP_DO_V	Connection	2)C5	0.05	Y	0.05	45%	0.0225	Y		0.00%	0.0225
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0.0000				
HV Measurement Inputs											
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	45%	0.0000				
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	45%	0.0000				
HV Measurement Internal											
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	45%	0.0000				
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0.0000				
S's'_HVPOS_AI_1V,HVPOS_BUS_A	Transducer	1)T2	14		0	45%	0.0000				
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	45%	0.0000				
Power Supply	General - PSU	1)PSU2	20		0	45%	0.0000				
HV Measurement Outputs											
S's'_HVPOS_AI_1V	Data	1)D7	3		0	45%	0.0000				
String Management Inputs											
M'm'_TRIP_DO_V	Connection	2)C6	0.05	Y	0.05	45%	0.0225	Y		0.00%	0.0225
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0.0000				
String Management Internal											
SAFETY_OK_DI_V	Measurement	2)M5	4	Y	4	45%	1.8000	Y		0.00%	1.8
M'm'_OK_DLY_DI_V	Transducer	2)T4	8	Y	8	45%	3.6000	Y		0.00%	3.6
Power Supply	General - PSU	1)PSU3	10	Y	10	45%	4.5000	Y			4.5
String Management Outputs											
HVPOS1P_DHSO	Output	1)O1	20		0	45%	0.0000			0.00%	
HVNEGN_DLO_V	Output	1)O2	20	Y	20	45%	9.0000	Y		0.00%	9
String Hardware Logic Inputs											
M'm'_OK_DLY_DI_V	Actuator	2)A6	15	Y	15	45%	6.7500	Y	Refer to element reference	0.00%	6.75
String Hardware Logic outputs											
HVPOS1N_DLO_V	Output	2)O5	20		0	45%	0.0000			0.00%	
HVNEGP_DHO_V	Output	2)O6	20	Y	20	45%	9.0000	Y			9
Coils											
HVPOS1N_DHSO	Actuator	2)A4	30		0	100%	0.0000			0.00%	
HVNEGP_DHSO	Actuator	2)A7	30	Y	30	100%	30.0000	Y			30
			505.15		**206.25**			**SPFM =**	**63.0%**		**76.38**

Table 60: Maintain OA Architecture 2 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %		Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Failure Mode coverage with respect to Latent failures, %	Latent multiple-Point failure rate/FIT
Connections													
C'c'_AI_0V001	Connection	2)C1	0.6	Y	0.6	45%	0.1944	Y	100.00%	0.1944			0.1944
C'c'_AI_0V	Connection	2)C2	0.05	Y	0.05	45%	0.0162	Y	100.00%	0.0162			0.0162
HW Monitor													
C'c'_AI_0V001	Measurement	2)M3	24	Y	24	45%	7.00164	y	100.00%	7.0016			7.00164
C'c'_AI_0V001	Transducer	2)T3	25	Y	25	45%	8.178384375	y	100.00%	8.1784			8.178384375
SPI ADC Inputs													
C'c'_AI_0V001	Measurement	2)M1	102		0	45%	0			0.0000			
SPI ADC Internal													
VMEAS_AI_TX	Transducer	1)T1	50		0	45%	0			0.0000			
SPI ADC Outputs													
VMEAS_AI_TX	Data	1)D1	3		0	45%	0			0.0000			
Module Management Inputs													
VMEAS_AI_TX	Data	1)D2	3		0	45%	0			0.0000			
M'm'_TRIP_FO_1Hz	Measurement	2)M4	3.5	Y	3.5	45%	1.575			0.0000			
Module Management Internals													
C'c'_AI_0V001	Parameter	1)P1	4.5		0	45%	0			0.0000			
C'c'_OA_0V001	Parameter	1)P2	4.5		0	45%	0			0.0000			
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	45%	0.44226	Y	100.00%	0.4423			0.44226
M'm'_TRIP_DI_V	Output	2)O3	25	Y	25	45%	6.6555	Y	100.00%	6.6555			6.6555
Power Supply	General - PSU	1)PSU1	20	Y	20	45%	8.86545	Y	100.00%	8.8655			8.86545
Module Management Outputs													
M'm'_TRIP_DO_V	Connection	2)C5	0.05	Y	0.05	45%	0			0.0000			
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
HV Measurement Inputs													
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	45%	0			0.0000			
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	45%	0			0.0000			
HV Measurement Internal													
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	45%	0			0.0000			
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,HVPOS_BUS_A	Transducer	1)T2	14		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	45%	0			0.0000			
Power Supply	General - PSU	1)PSU2	20		0	45%	0			0.0000			
HV Measurement Outputs													
S's'_HVPOS_AI_1V	Data	1)D7	3		0	45%	0			0.0000			
String Management Inputs													
M'm'_TRIP_DO_V	Connection	2)C6	0.05	Y	0.05	45%	0			0.0000			
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
String Management Internal													
SAFETY_OK_DI_V	Measurement	2)M5	4	Y	4	45%	0	Y	100.00%	0.0000			0
M'm'_OK_DLY_DI_V	Transducer	2)T4	8	Y	8	45%	0	Y	100.00%	0.0000			0
Power Supply	General - PSU	1)PSU3	10	Y	10	45%	0	Y	100.00%	0.0000			0
String Management Outputs													
HVPOS1P_DHSO	Output	1)O1	20		0	45%	0			0.0000			
HVNEGN_DLO_V	Output	1)O2	20	Y	20	45%	0	y	100.00%	0.0000			0
String Hardware Logic Inputs													
M'm'_OK_DLY_DI_V	Actuator	2)A6	15	Y	15	45%	0	y	100.00%	0.0000			0
String Hardware Logic outputs													
HVPOS1N_DLO_V	Output	2)O5	20		0	45%	0			0.0000			
HVNEGP_DHO_V	Output	2)O6	20	Y	20	45%	0	y	100.00%	0.0000			0
Coils													
HVPOS1N_DHSO	Actuator	2)A4	30		0	100%	0			0.0000			
HVNEGP_DHSO	Actuator	2)A7	30	Y	30	100%	0	y	100.00%	0.0000			0
			505.15		**206.25**		**LFM =**	**75.9%**					**31.35**

As expected this results in a reduction in the SPFM percentage from 81.6% to 63% as implementation of the diagnostic functionality is harder to achieve in hardware and, as in architecture 1, this is a functional implementation rather than one targeted to specifically address functional safety. The increase in LFM is largely due to the increase in single point faults (as indicated by the lower SPFM).

This highlights another important aspect of the PCc method. When starting a new project, several approaches have to be taken into account. For a full production intent design then there is no doubt that a full design lifecycle process (including the application of BS ISO 26262 guidelines) must be followed. However, in an early proof of concept design, a compromise can be made between

allocation of safety aspects to hardware or software. For example, there may be less effort in designing a hardware safety monitor around a system that ensures safety is achieved, irrespective of actions taken in the software. This may provide software / controls engineers greater scope to develop innovative ideas / test new algorithms without the onerous task of validating each new control concept with the knowledge that the system will always be safe due to hardware detection and shutdown methods. As the system is developed, a decision can be made to reduce hardware costs (a cost per unit) and move safety into the software with the associated validation / verification costs which can be amortised over the production volume. The PCc method gives a route to assess the approaches in a quantified way.

The logical approach to progress this architecture is to combine the software and hardware to improve diagnostic coverage and hence increase the architectural metrics.

4.3.6.11 Cell Voltage Operating Area – Architecture 3

Measurement of the cell voltages using a combination of an accurate (AFE) as discussed in 4.3.6.1 with a diverse hardware shutoff mechanism (Figure 25). This is expected to provide improved diagnostics as there are now effectively two monitoring systems, one in software and one in hardware.

Accurate measurements are now available for accurate control of the cell voltages but if this system fails a hardware shutoff mechanism will deploy rendering the system into a safe state.

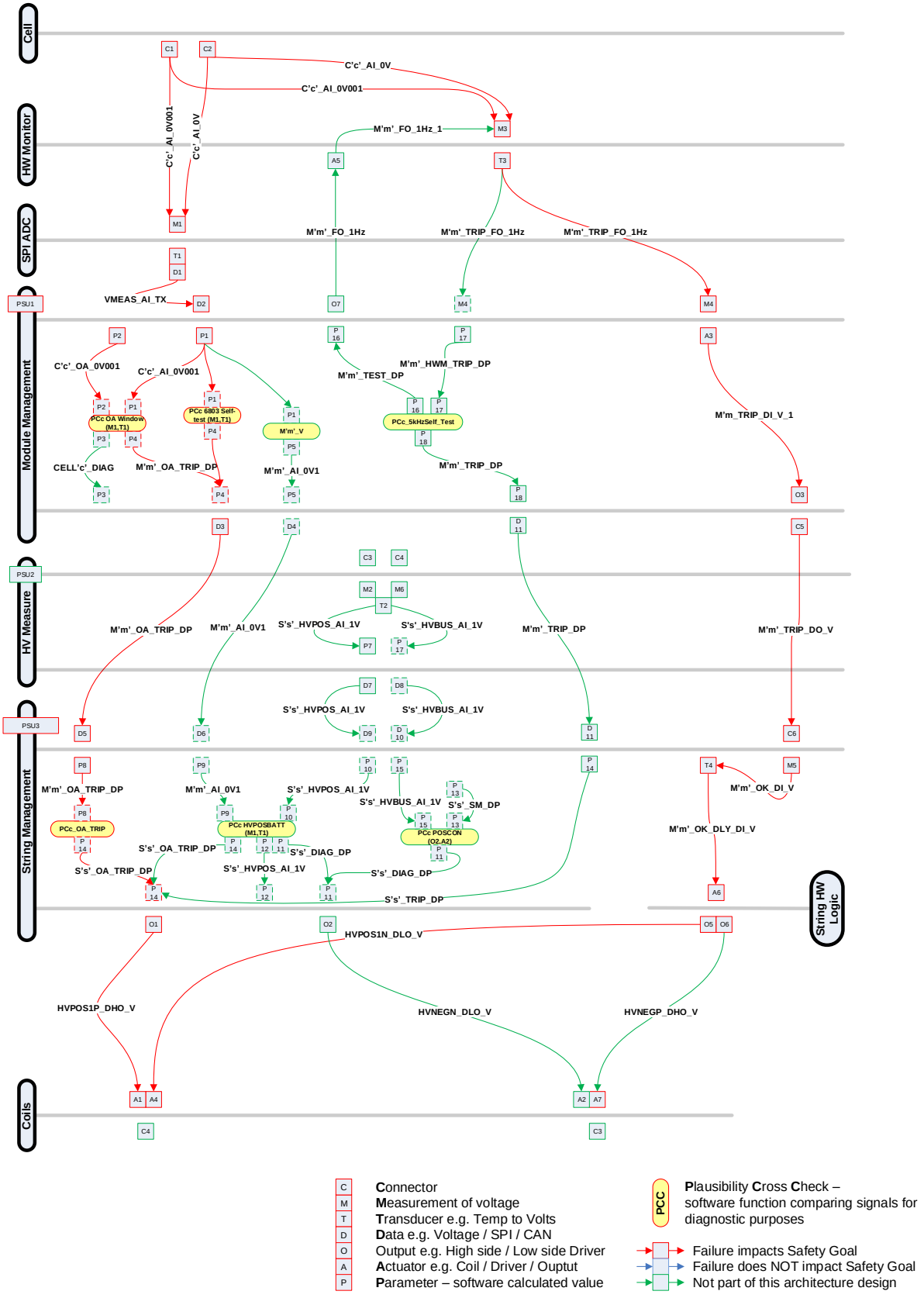


Figure 25: Maintain OA - Concept Architecture Candidate 3

4.3.6.12 Cell Voltage Operating Area – Architecture 3 Classified Signals

All of the element signals used in Architecture Candidate 3 (Figure 25) have been discussed previously, no new signals are used but the signals from Architecture 1 (4.3.6.2) and Architecture 2 (4.3.6.7) are combined.

4.3.6.13 Cell Voltage Operating Area – Architecture 3 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.3.6.14. Table 61 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 61: BMS Architecture 3 Element Cross Reference to Diagnostic Coverage Claims

Element	**Diagnostic Coverage Calculation Table Reference in Appendix E3 – BMS – Architecture 3 DC% Claims**
3)T3	Table 147: BMS - Architecture 3 Transducer 3

4.3.6.13.1 Element '3)T3'

The PCc6801_Self_Test (4.3.6.9.3) is now confirmed by on-line monitoring as the data is also available from the LTC6803 AFE.

4.3.6.14 Cell Voltage Operating Area – Architecture 3 Plausibility Cross-checks

No additional PCcs are used, however the integrity of the self-tests is improved.

4.3.6.15 Cell Voltage Operating Area – Architecture 3 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 62 and the LFM calculation shown in Table 63.

Table 62: Maintain OA Architecture 3 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Failure mode that has the potential to violate the SG in the absense of a Safety Mechanism	Safety mechanisms allowing to prevent violation of Safety Goal
Connections								
C'c'_AI_0V001	Connection	1)C1	0.6	Y	0.6	45%	Y	PCc_6803_Self_Test
C'c'_AI_0V	Connection	1)C2	0.05	Y	0.05	45%	Y	PCc_6803_Self_Test
HW Monitor								
C'c'_AI_0V001	Measurement	2)M3	24	Y	24	45%	Y	PCc6801_Self_-Test
C'c'_AI_0V001	Transducer	3)T3	25	Y	25	45%	Y	6801 Internal functionality, Don't claim 5kHz as not independently proved to be periodic. PCc_PSU_Mon
BATT'b'_PO_PC	Actuator	A5			0	45%		
SPI ADC Inputs								
C'c'_AI_0V001	Measurement	2)M1	102	Y	102	45%	Y	OA Window, PCc_6803_Self_Test
SPI ADC Internal								
VMEAS_AI_TX	Transducer	1)T1	50	Y	50	45%	Y	PCc_OA_Window, PCc_6803_Self_Test, PCc_PSU_Mon
SPI ADC Outputs								
VMEAS_AI_TX	Data	1)D1	3	Y	3	45%	Y	PCc_Data_Checksum, PCc_Poll_Response_Time
Module Management Inputs								
VMEAS_AI_TX	Data	1)D2	3	Y	3	45%	Y	PCc_Data_Checksum, PCc_Poll_Response_Time
M'm'_TRIP_FO_1Hz	Measurement	2)M4	3.5	Y	3.5	45%	Y	
Module Management Internals								
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	45%	Y	PCc_RAM_Test, PCc_Code_Sea, PCc_Micro_Test, PCc_PSU_Mon
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	45%	Y	PCc_RAM_Test, PCc_Code_Sea, PCc_Micro_Test, PCc_PSU_Mon
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	45%	Y	PCc_PSU_Mon
M'm'_TRIP_DI_V	Output	2)O3	25	Y	25	45%	Y	PCc_PSU_Mon, PCC_OA_TRIP
Power Supply	General - PSU	1)PSU1	60	Y	60	45%	Y	PCc_PSU_Mon
Module Management Outputs								
M'm'_OA_TRIP_DP	Data	1)D3	3	Y	3	45%	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time
M'm'_TRIP_DO_V	Connection	2)C5	0.05	Y	0.05	45%	Y	
M'm'_TRIP_DP	Data	4)D11	3		0	45%		
HV Measurement Inputs								
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	45%		
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	45%		
HV Measurement Internal								
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	45%		
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%		
S's'_HVPOS_AI_1V,HVPOS_BUS_	Transducer	1)T2	14		0	45%		
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	45%		
Power Supply	General - PSU	1)PSU2	40		0	45%		
HV Measurement Outputs								
S's'_HVPOS_AI_1V	Data	1)D7	3		0	45%		
String Management Inputs								
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	45%	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time
M'm'_TRIP_DO_V	Connection	2)C6	0.05	Y	0.05	45%	Y	
M'm'_TRIP_DP	Data	4)D11	3		0	45%		
String Management Internal								
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	45%	Y	PCc_RAM_Test, PCc_Code_Sea, PCc_Micro_Test, PCc_PSU_Mon
SAFETY_OK_DI_V	Measurement	2)M5	4	Y	4	45%	Y	
M'm'_OK_DLY_DI_V	Transducer	2)T4	8	Y	8	45%	Y	PCc_PSU_Mon
Power Supply	General - PSU	1)PSU3	40	Y	40	45%	Y	PCc_PSU_Mon
String Management Outputs								
HVPOS1P_DHO_V	Output	1)O1	20	Y	20	45%	Y	PCc_PSU_Mon
HVNEGN_DLO_V	Output	1)O2	20		0	45%		
String Hardware Logic Inputs								
M'm'_OK_DLY_DI_V	Actuator	2)A6	12	Y	12	45%	Y	PCc_PSU_Mon
String Hardware Logic outputs								
HVPOS1N_DLO_V	Output	2)O5	20	Y	20	45%	Y	PCc_PSU_Mon
HVNEGP_DHO_V	Output		20	Y	20	45%	Y	PCc_PSU_Mon
Coils								
HVPOS1P_DHO_V	Actuator	1)A1	15	Y	15	100%	Y	PCc_PSU_Mon
HVPOS1N_DHSO	Actuator	2)A4	15	Y	15	100%	Y	PCc_PSU_Mon
HVNEGN_DLO_V	Actuator	1)A2	15	Y	15	100%	Y	
HVNEGP_DHO_V	Actuator	2)A7	15	Y	15	100%	Y	PCc_PSU_Mon
			610.15		**508.25**		**SPFM =**	**77.6%**

Table 63: Maintain OA Architecture 3 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %		Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Failure Mode coverage with respect to Latent failures, %	Latent.multiple-Point failure rate/FIT
Connections													
C'c'_AI_0V001	Connection	1)C1	0.6	Y	0.6	45%	0.1134	Y	100.00%	0.1134	PCc6801_Self_Test partia	10.00%	0.10206
C'c'_AI_0V	Connection	1)C2	0.05	Y	0.05	45%	0.0162	Y	100.00%	0.0162	PCc6801_Self_Test partia	10.00%	0.01458
HW Monitor													
C'c'_AI_0V001	Measurement	2)M3	24	Y	24	45%	7.00164	y	100.00%	7.0016			7.00164
C'c'_AI_0V001	Transducer	3)T3	25	Y	25	45%	8.178384375	y	100.00%	8.1784			8.178384375
BATT'b'_PO_PC	Actuator	A5			0	45%	0	y	100.00%	0.0000			0
SPI ADC Inputs													
C'c'_AI_0V001	Measurement	2)M1	102	Y	102	45%	45.080145	y	100.00%	45.0801	PCc6801_Self_Test partia	10.00%	40.5721305
SPI ADC Internal													
VMEAS_AI_TX	Transducer	1)T1	50	Y	50	45%	21.99099375	y	100.00%	21.9910	PCc6801_Self_Test partia	10.00%	19.79189438
SPI ADC Outputs													
VMEAS_AI_TX	Data	1)D1	3	Y	3	45%	1.225692	Y	100.00%	1.2257	PCc6801_Self_Test partia	10.00%	1.1031228
Module Management Inputs													
VMEAS_AI_TX	Data	1)D2	3	Y	3	45%	1.225692	Y	100.00%	1.2257	PCc6801_Self_Test partia	10.00%	1.1031228
M'm'_TRIP_FO_1Hz	Measurement	2)M4	3.5	Y	3.5	45%	0	Y	100.00%	0.0000			0
							0						
Module Management Internals													
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	45%	1.905069375	Y	100.00%	1.9051	Wdog	90.00%	0.190506938
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	45%	1.911027938	Y	100.00%	1.9110	Wdog	90.00%	0.191102794
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	45%	0.44226	Y	100.00%	0.4423			0.44226
M'm'_TRIP_DI_V	Output	2)O3	25	Y	25	45%	6.6555	Y	100.00%	6.6555			6.6555
Power Supply	General - PSU	1)PSU1	60	Y	60	45%	26.59635	Y	100.00%	26.5964	Wdog	90.00%	2.659635
Module Management Outputs													
M'm'_OA_TRIP_DP	Data	1)D3	3	Y	3	45%	1.296405	Y	100.00%	1.2964	PCc6801_Self_Test partia	10.00%	1.1667645
M'm'_TRIP_DO_V	Connection	2)C5	0.05	Y	0.05	45%	0			0.0000			
							0						
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
HV Measurement Inputs													
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	45%	0			0.0000			
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	45%	0			0.0000			
HV Measurement Internal													
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	45%	0			0.0000			
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,HVPOS_BUS_A	Transducer	1)T2	14		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	45%	0			0.0000			
Power Supply	General - PSU	1)PSU2	40		0	45%	0			0.0000			
HV Measurement Outputs													
S's'_HVPOS_AI_1V	Data	1)D7	3		0	45%	0			0.0000			
String Management Inputs													
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	45%	2.59281	Y	100.00%	2.5928	PCc6801_Self_Test partia	10.00%	2.333529
M'm'_TRIP_DO_V	Connection	2)C6	0.05	Y	0.05	45%	0			0.0000			
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
String Management Internal													
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	45%	3.81013875	Y	100.00%	3.8101	Wdog	90.00%	0.381013875
SAFETY_OK_DI_V	Measurement	2)M5	4	Y	4	45%	0	Y	100.00%	0.0000			0
M'm'_OK_DLY_DI_V	Transducer	2)T4	8	Y	8	45%	0	Y	100.00%	0.0000			0
Power Supply	General - PSU	1)PSU3	40	Y	40	45%	17.7309	Y	100.00%	17.7309	Wdog	90.00%	1.77309
String Management Outputs													
HVPOS1P_DHO_V	Output	1)O1	20	Y	20	45%	0	Y	100.00%	0.0000	PCc6801_Self_Test partia	10.00%	0
HVNEGN_DLO_V	Output	1)O2	20		0	45%	0	y	100.00%	0.0000			0
String Hardware Logic Inputs													
M'm'_OK_DLY_DI_V	Actuator	2)A6	12	Y	12	45%	0	y	100.00%	0.0000			0
String Hardware Logic outputs													
HVPOS1N_DLO_V	Output	2)O5	20	Y	20	45%	0	y	100.00%	0.0000			0
HVNEGP_DHO_V	Output		20	Y	20	45%	0	y	100.00%	0.0000			0
Coils													
HVPOS1P_DHO_V	Actuator	1)A1	15	Y	15	100%	0	Y	100.00%	0.0000	PCc6801_Self_Test partia	10.00%	0
HVPOS1N_DHSO	Actuator	2)A4	15	Y	15	100%	0	y	100.00%	0.0000			0
HVNEGN_DLO_V	Actuator	1)A2	15	Y	15	100%	0	y	100.00%	0.0000			0
HVNEGP_DHO_V	Actuator	2)A7	15	Y	15	100%	0	y	100.00%	0.0000			0
			610.15		**508.25**		**LFM =**	**76.2%**					**93.66**

This significantly increases the SPFM over the hardware only design but now that we have an increase in hardware componentry over the original software design the SPFM is lower than Architecture 1. This is considered acceptable as the design now offers a number of advantages:

1) Accurate monitoring and control can be achieved in software, the vehicle driver warned as cell capacity approaches minimum and a controlled system shutdown actioned in software, if required.
2) There is an independent backup; if the software fails to shut down the system in a controlled way, the hardware can act and shut down the system. This would not be as controlled but would render the system safe.

The LFM has improved over both earlier designs as expected as we now have two independent systems.

4.3.6.16 Cell Voltage Operating Area – Architecture 4

Architecture 4 improves detection of any failures in the battery microcontroller by utilising a 5kHz signal generated by the microcontroller to drive the hardware shutoff mechanism (Figure 26). If this signal fails then the hardware mechanism will shut down the system irrespective of when the cell voltages had deviated from their normal operating area. By ensuring that the battery microcontroller only generates this 5kHz signal if it is running correctly, any diagnosable critical faults in the microcontroller can independently shut down the system. One such case would be when the battery microcontroller determined that the operating area had been exceeded, the string controller notified but the string controller but the system hadn't taken the appropriate action. The 5kHz signal also has a self-test facility so that the output of the hardware shut off mechanism can be monitored in the trip state when the 5 kHz is not present.

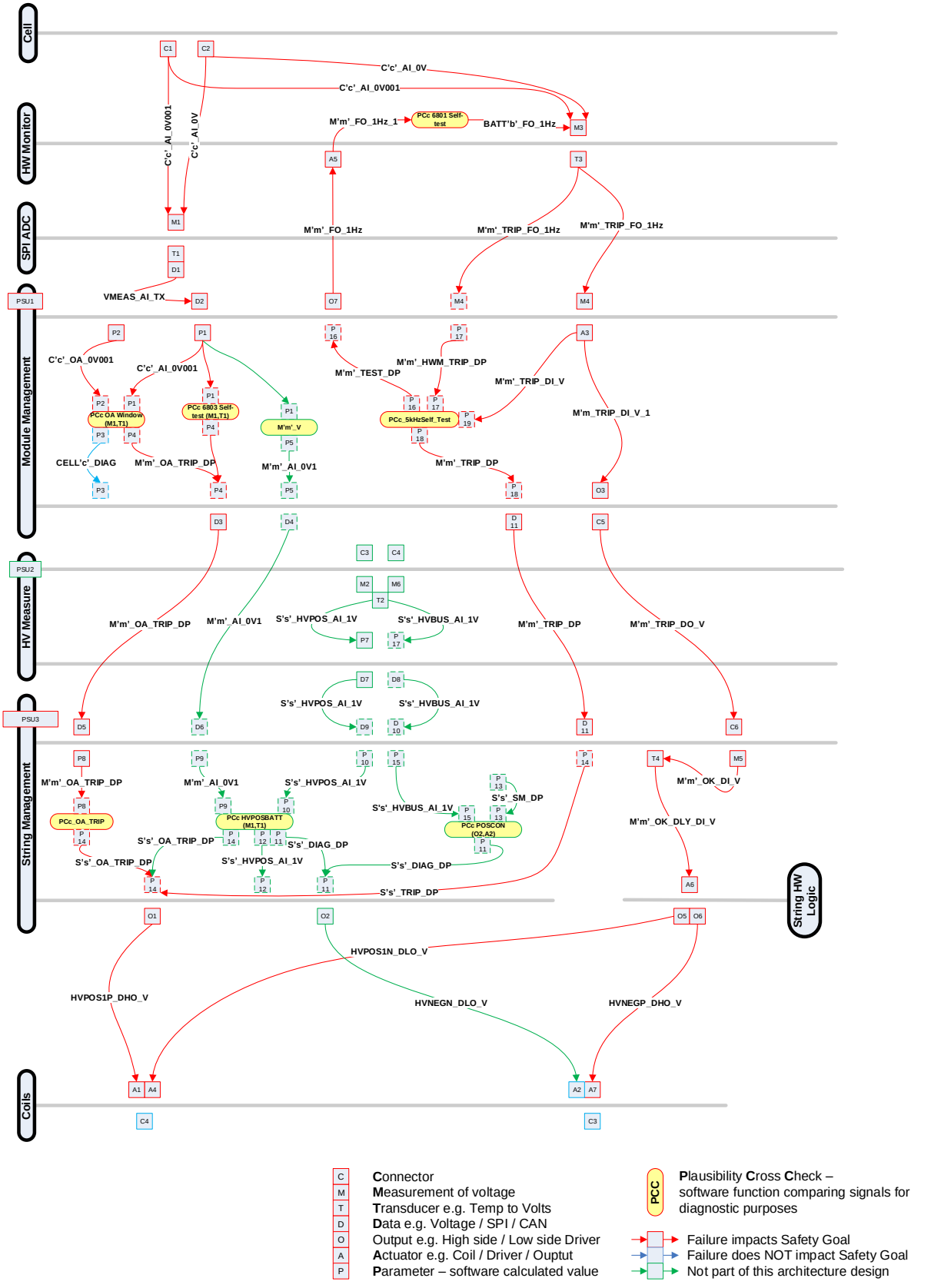


Figure 26: Maintain OA - Concept Architecture Candidate 4

4.3.6.17 Cell Voltage Operating Area – Architecture 4 Classified Signals

All of the signals used in Architecture Candidate 4 (Figure 26) that have been discussed previously are not duplicated in this section. Only new signals or those with increased diagnostic coverage are discussed.

4.3.6.17.1 HW Monitor

4.3.6.17.1.1 A5 – M'm'_FO_1Hz_1

The hardware monitor uses the M'm'_FO_1Hz_1 signal as a clock input to the hardware monitor (LTC6803).

4.3.6.17.2 SPI ADC Inputs

4.3.6.17.3 Module Management Inputs

4.3.6.17.3.1 M4 – M'm'_TRIP_FO_1Hz

The measurement of the trip signal based on the hardware monitor transducer output.

4.3.6.17.4 Module Management Internals

4.3.6.17.4.1 P16 - M'm'_TEST_DP

The signal M'm'_TEST_DP is the internal parameter value used to control the output.

4.3.6.17.4.2 P17 – M'm'_HWM_TRIP_DP

The internal parameter that indicates that the hardware monitor has tripped.

4.3.6.17.4.3 P18 - M'm'_TRIP_DP

The signal M'm'_TRIP_DP used to indicate to the String Management system that the hardware monitor has tripped.

4.3.6.17.5 Module Management Outputs

4.3.6.17.5.1 O7 - M'm'_FO_1Hz

The signal M'm_TEST_DP is used to determine the value of the output in Hz. In this example it is assumed that this is bi-state 0 Hz or 5 kHz. Theoretically, additional diagnostics can be performed by varying this signal frequency and duty cycle to ensure correct operation of the hardware monitor (LTC6801).

4.3.6.17.5.2 D11 - M'm'_TRIP_DP

The signal M'm'_TRIP_DP transmitted from the Module Management CAN Bus interface.

4.3.6.17.6 String Management Inputs

4.3.6.17.6.1 D11 - M'm'_TRIP_DP

M'm'_TRIP_DP received at the String Management CAN bus interface.

4.3.6.17.7 String Management Internal

4.3.6.17.7.1 P14 – S's'_TRIP_DP / S's'_OA_TRIP_DP

An internal parameter that indicates that the string has tripped. This uses a combination of signals. M'm'_TRIP_DP is monitored for each module in turn and if any module has tripped (exceeded the operating area window for a given voltage profile) as determined by the hardware monitor then the string trip flag will be set (S's_TRIP_DP).

This can be further modified by the operating area trip S's_OA_TRIP_DP (software controlled) which is set if any one of the modules has exceeded is voltage / temperature profile (M'm_OA_TRIP_DP).

4.3.6.18 Cell Voltage Operating Area – Architecture 4 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.3.6.19. Table 64 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 64: BMS Architecture 4 Element Cross Reference to Diagnostic Coverage Claims

Element	Diagnostic Coverage Calculation Table Reference in Appendix E4 – BMS – Architecture 4 DC% Claims
4)A5	Table 148: BMS - Architecture 4 Actuator 5
4)D11	Table 149: BMS - Architecture 4 Data 11 (subset 1) Table 150: BMS - Architecture 4 Data 11 (subset 2)
4)M4	Table 151: BMS - Architecture 4 Measurement 4
4)O7	Table 152: BMS - Architecture 4 Output 7

4.3.6.18.1 Element '4)A5'

This drives the differential actuator to the LTC6801. This converts the differential input into the clock that is used by the hardware monitor to run the LTC6801. A limited amount of test can now be achieved by the PCc_5kHzSelf_Test (4.3.6.9.2).

4.3.6.18.1 Element '4)D11'

This is the status of the hardware monitor trip output from the module management to the string management. As this is over CAN the diagnostics are comprehensive.

4.3.6.18.2 Element '4)M4'

Diagnostics is now improved for this input as the PCc_5kHzSelf_Test (4.3.6.9.2) itself is monitored. There is some limitation in that this is all contained within the Module Management system i.e. no independence.

4.3.6.18.1 Element '4)O7'

The differential output from the microcontroller. This output can now be validated by the PCc_5kHzSelf_Test (4.3.6.9.2). Also, it is a differential output from the microcontroller and so additional integrity is provided by the configuration of the microcontroller. This allows one output to be driven by the monitoring software in the microcontroller (i.e. only driven when the safety monitoring software is valid) and the other output can be driven by the normal control software.

4.3.6.19 Cell Voltage Operating Area – Architecture 4 Plausibility Cross-checks

No additional Plausibility checks are introduced in this architecture.

4.3.6.20 Cell Voltage Operating Area – Architecture 4 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 65 and the LFM calculation shown in Table 66.

Table 65: Maintain OA Architecture 4 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %		Failure mode that has the potential to violate the SG in the absense of a Safety Mechanism	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Connections											
C'c'_AI_0V001	Connection	1)C1	0.6	Y	0.6	45%	0.2700	Y	PCc_6803_Self_Test	42.00%	0.1566
C'c'_AI_0V	Connection	1)C2	0.05	Y	0.05	45%	0.0225	Y	PCc_6803_Self_Test	72.00%	0.0063
HW Monitor											
C'c'_AI_0V001	Measurement	2)M3	24	Y	24	45%	10.8000	Y	PCc6801_Self_Test, PCc_5kHzSelft_Test	64.83%	3.79836
C'c'_AI_0V001	Transducer	3)T3	25	Y	25	45%	11.2500	Y	6801 internal functionality, Don't claim 5kHz as not independently proved to be periodic. PCc_PSU_Mon	72.70%	3.071615625
BATT'b'_PO_PC	Actuator	4)A5	0.5		0	45%	0.0000				
SPI ADC Inputs											
C'c'_AI_0V001	Measurement	2)M1	102	Y	102	45%	45.9000	Y	PCc_OA_Window, PCc_6803_Self_Test	98.21%	0.819855
SPI ADC Internal											
VMEAS_AI_TX	Transducer	1)T1	50	Y	50	45%	22.5000	Y	PCc_OA_Window, PCc_6803_Self_Test	97.74%	0.50900625
SPI ADC Outputs											
VMEAS_AI_TX	Data	1)D1	3	Y	3	45%	1.3500	Y	PCc_Data_Checksum, PCc_Poll_Response_Time	90.79%	0.124308
Module Management Inputs											
VMEAS_AI_TX	Data	1)D2	3	Y	3	45%	1.3500	Y	PCc_Data_Checksum, PCc_Poll_Response_Time	90.79%	0.124308
M'm'_TRIP_FO_1Hz	Measurement	4)M4	3.5	Y	3.5	45%	1.5750	Y	PCc_5kHzSelft_Test	44.64%	0.87192
Module Management Internals											
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	45%	2.0250	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW selftest	94.08%	0.119930625
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	45%	2.0250	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW selftest, CRC on CAL Tables	94.37%	0.113972063
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	45%	0.4500	Y	PCc_PSU_Mon, PCc_5kHzSelft_Test	98.28%	0.00774
M'm'_TRIP_DI_V	Output	2)O3	25	Y	25	45%	11.2500	Y	PCc_PSU_Mon, PCC_OA_TRIP	59.16%	4.5945
Power Supply	General - PSU	1)PSU1	60	Y	60	45%	27.0000	Y	PCc_PSU_Mon	98.51%	0.40365
Module Management Outputs											
M'm'_OA_TRIP_DP	Data	1)D3	3	Y	3	45%	1.3500	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.053595
M'm'_TRIP_DO_V	Connection	2)C5	0.05	Y	0.05	45%	0.0225	Y		0.00%	0.0225
BATT'b'_PO_PC	Output	4)O7	0.5		0	45%	0.0000		PCc_5kHzSelf_Test	97.52%	
M'm'_TRIP_DP	Data	4)D11	3	Y	3	45%	1.3500	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.053595
HV Measurement Inputs											
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	45%	0.0000				
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	45%	0.0000				
HV Measurement Internal											
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	45%	0.0000				
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0.0000				
S's'_HVPOS_AI_1V,HVPOS_BUS_A	Transducer	1)T2	14		0	45%	0.0000				
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	45%	0.0000				
Power Supply	General - PSU	1)PSU2	20		0	45%	0.0000				
HV Measurement Outputs											
S's'_HVPOS_AI_1V	Data	1)D7	3		0	45%	0.0000				
String Management Inputs											
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	45%	2.7000	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.10719
M'm'_TRIP_DO_V	Connection	2)C6	0.05	Y	0.05	45%	0.0225	Y		0.00%	0.0225
M'm'_TRIP_DP	Data	4)D11	3	Y	3	45%	1.3500	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.053595
String Management Internal											
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	45%	4.0500	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW selftest	94.08%	0.23986125
SAFETY_OK_DI_V	Measurement	2)M5	4	Y	4	45%	1.8000	Y		0.00%	1.8
M'm'_OK_DLY_DI_V	Transducer	2)T4	8	Y	8	45%	3.6000	Y	PCc_PSU_Mon	0.00%	3.6
Power Supply	General - PSU	1)PSU3	40	Y	40	45%	18.0000	Y	PCc_PSU_Mon	98.51%	0.2691
String Management Outputs											
HVPOS1P_DHO_V	Output	1)O1	20	Y	20	45%	9.0000	Y	PCc_PSU_Mon	0.00%	9
HVNEGN_DLO_V	Output	1)O2	20		0	45%	0.0000				
String Hardware Logic Inputs											
M'm'_OK_DLY_DI_V	Actuator	2)A6	12	Y	12	45%	5.4000	Y	PCc_PSU_Mon	0.00%	5.4
String Hardware Logic outputs											
HVPOS1N_DLO_V	Output	2)O5	20	Y	20	45%	9.0000	Y		0.00%	9
HVNEGP_DHO_V	Output	2)O6	20	Y	20	45%	9.0000	Y		0.00%	9
Coils											
HVPOS1P_DHO_V	Actuator	1)A1	15	Y	15	100%	15.0000	Y	PCc_PSU_Mon	0.00%	15
HVPOS1N_DHSO	Actuator	2)A4	15	Y	15	100%	15.0000	Y	PCc_PSU_Mon	0.00%	15
HVNEGN_DLO_V	Actuator	1)A2	15	Y	15	100%	15.0000	Y			15
HVNEGP_DHO_V	Actuator	2)A7	15	Y	15	100%	15.0000	Y	PCc_PSU_Mon	0.00%	15
			591.15		**514.25**			**SPFM =**	**78.0%**		**113.34**

Table 66: Maintain OA Architecture 4 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %		Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Failure Mode coverage with respect to Latent failures, %	Latent multiple-Point failure rate/FIT
Connections													
C'c'_AI_0V001	Connection	1)C1	0.6	Y	0.6	45%	0.1134	Y	100.00%	0.1134	PCc_HW_MONITOR with	30.00%	0.07938
C'c'_AI_0V	Connection	1)C2	0.05	Y	0.05	45%	0.0162	Y	100.00%	0.0162	PCc_HW_MONITOR with	30.00%	0.01134
HW Monitor													
C'c'_AI_0V001	Measurement	2)M3	24	Y	24	45%	7.00164	y	100.00%	7.0016			7.00164
C'c'_AI_0V001	Transducer	3)T3	25	Y	25	45%	8.178384375	y	100.00%	8.1784			8.178384375
BATT'b'_PO_PC	Actuator	4)A5	0.5		0	45%	0	y	100.00%	0.0000			0
SPI ADC Inputs													
C'c'_AI_0V001	Measurement	2)M1	102	Y	102	45%	45.080145	Y	100.00%	45.0801	PCc_HW_MONITOR with	30.00%	31.5561015
SPI ADC Internal													
VMEAS_AI_TX	Transducer	1)T1	50	Y	50	45%	21.99099375	Y	100.00%	21.9910	PCc_HW_MONITOR with	30.00%	15.39369563
SPI ADC Outputs		**3**		**45%**		3			**1.225692**				
VMEAS_AI_TX	Data	1)D1	3	Y	3	45%	1.225692	Y	100.00%	1.2257	PCc_HW_MONITOR with	30.00%	0.8579844
Module Management Inputs													
VMEAS_AI_TX	Data	1)D2	3	Y	3	45%	1.225692	Y	100.00%	1.2257	PCc_HW_MONITOR with	30.00%	0.8579844
M'm'_TRIP_FO_1Hz	Measurement	4)M4	3.5	Y	3.5	45%	0.70308	Y	100.00%	0.7031	Wdog	90.00%	0.070308
							0						
Module Management Internals													
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	45%	1.905069375	Y	100.00%	1.9051	Wdog	90.00%	0.190506938
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	45%	1.911027938	Y	100.00%	1.9110	Wdog	90.00%	0.191102794
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	45%	0.44226	Y	100.00%	0.4423			0.44226
M'm'_TRIP_DI_V	Output	2)O3	25	Y	25	45%	6.6555	Y	100.00%	6.6555			6.6555
Power Supply	General - PSU	1)PSU1	60	Y	60	45%	26.59635	Y	100.00%	26.5964	Wdog	90.00%	2.659635
Module Management Outputs													
M'm'_OA_TRIP_DP	Data	1)D3	3	Y	3	45%	1.296405	Y	100.00%	1.2964	PCc_HW_MONITOR with	30.00%	0.9074835
M'm'_TRIP_DO_V	Connection	2)C5	0.05	Y	0.05	45%	0			0.0000			
BATT'b'_PO_PC	Output	4)O7	0.5		0	45%	0			0.0000			
M'm'_TRIP_DP	Data	4)D11	3	Y	3	45%	1.296405	Y	100.00%	1.2964			1.296405
HV Measurement Inputs													
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	45%	0			0.0000			
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	45%	0			0.0000			
HV Measurement Internal													
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	45%	0			0.0000			
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,HVPOS_BUS_A	Transducer	1)T2	14		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	45%	0			0.0000			
Power Supply	General - PSU	1)PSU2	20		0	45%	0			0.0000			
HV Measurement Outputs													
S's'_HVPOS_AI_1V	Data	1)D7	3		0	45%	0			0.0000			
String Management Inputs													
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	45%	2.59281	Y	100.00%	2.5928	PCc_HW_MONITOR with	30.00%	1.814967
M'm'_TRIP_DO_V	Connection	2)C6	0.05	Y	0.05	45%	0			0.0000			
M'm'_TRIP_DP	Data	4)D11	3	Y	3	45%	1.296405	Y	100.00%	1.2964			1.296405
String Management Internal													
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	45%	3.81013875	Y	100.00%	3.8101	Wdog	90.00%	0.381013875
SAFETY_OK_DI_V	Measurement	2)M5	4	Y	4	45%	0	Y	100.00%	0.0000			0
M'm'_OK_DLY_DI_V	Transducer	2)T4	8	Y	8	45%	0	Y	100.00%	0.0000			0
Power Supply	General - PSU	1)PSU3	40	Y	40	45%	17.7309	Y	100.00%	17.7309	Wdog	90.00%	1.77309
String Management Outputs													
HVPOS1P_DHO_V	Output	1)O1	20	Y	20	45%	0	Y	100.00%	0.0000	PCc_HW_MONITOR with	30.00%	0
HVNEGN_DLO_V	Output	1)O2	20		0	45%	0	y	100.00%	0.0000			0
String Hardware Logic Inputs													
M'm'_OK_DLY_DI_V	Actuator	2)A6	12	Y	12	45%	0	y	100.00%	0.0000			0
String Hardware Logic outputs													
HVPOS1N_DLO_V	Output	2)O5	20	Y	20	45%	0	y	100.00%	0.0000			0
HVNEGP_DHO_V	Output	2)O6	20	Y	20	45%	0	y	100.00%	0.0000			0
Coils													
HVPOS1P_DHO_V	Actuator	1)A1	15	Y	15	100%	0	Y	100.00%	0.0000	PCc_HW_MONITOR with	72.00%	0
HVPOS1N_DHSO	Actuator	2)A4	15	Y	15	100%	0	y	100.00%	0.0000			0
HVNEGN_DLO_V	Actuator	1)A2	15	Y	15	100%	0	y	100.00%	0.0000			0
HVNEGP_DHO_V	Actuator	2)A7	15	Y	15	100%	0	y	100.00%	0.0000			0
			591.15		**514.25**		**LFM =**	**79.6%**					**81.62**

A negligible increase in SPFM from 77.6% to 78% is achieved through the improvement in the self-test diagnostic coverage. The LFM also increases from 76.2% to 79.8% now that the hardware safety mechanism is tested i.e. it can be proved to work periodically rather than it being dormant and only called into action when required.

4.3.6.21 Cell Voltage Operating Area – Architecture 5

To improve the self-test on the 5kHz output the self-test function has been moved to the string controller (Figure 27). This means that the shut off mechanism can be tested through the Module Management microcontroller, the hardware shut off mechanism and back through to the logic in the string ECU.

The self-test is monitored through a safety timer (M'm'_SAFETY_TIME_DP) to ensure:

1) That the test is run periodically.
2) That the periodicity is correct within a tolerance.

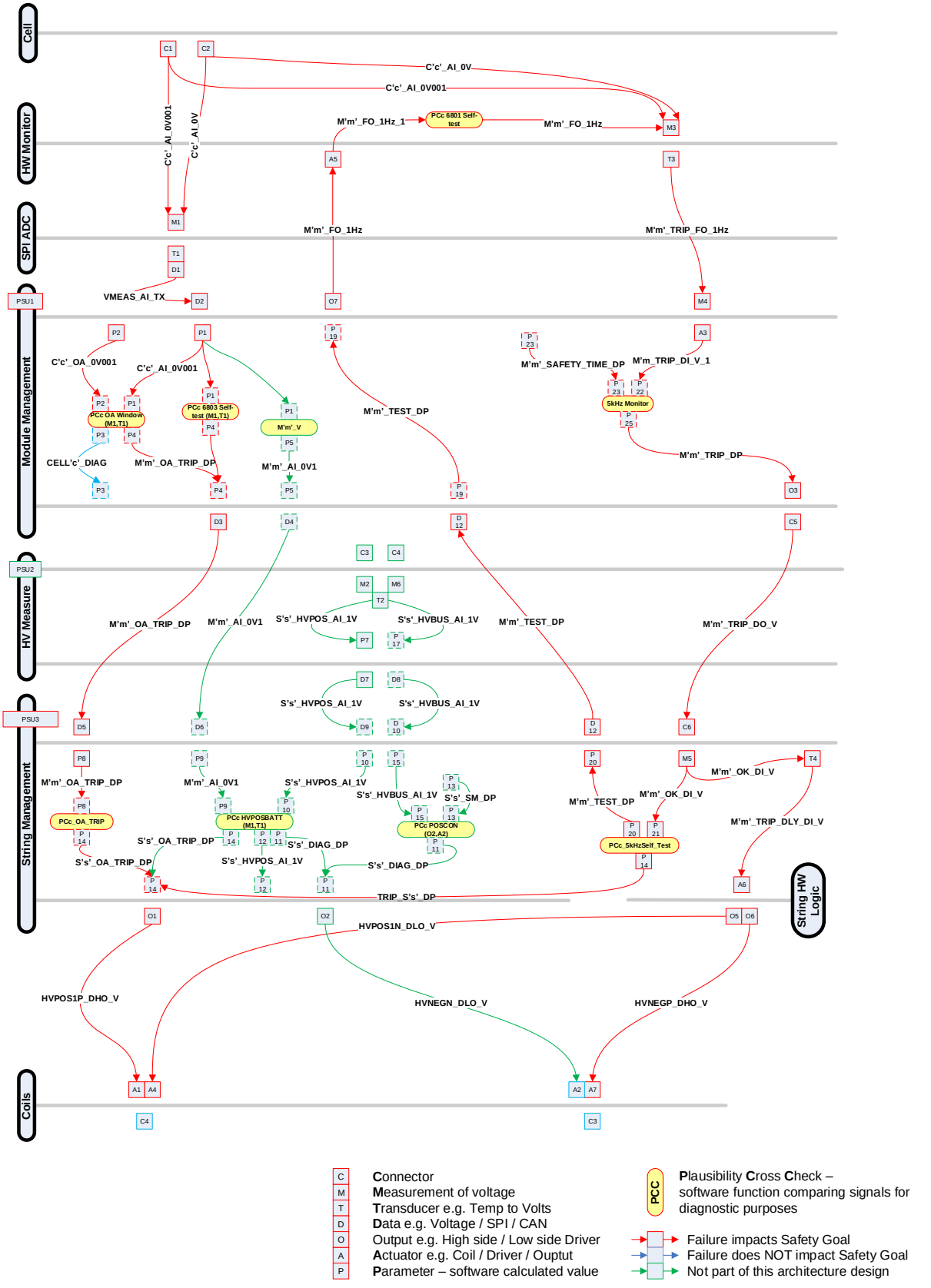


Figure 27: Maintain OA - Concept Architecture Candidate 5

4.3.6.22 Cell Voltage Operating Area – Architecture 5 Classified Signals

For clarity, only signals for this candidate architecture diagram (Figure 27) are discussed in this section. The relevant PCcs that are applied are discussed in subsequent sections.

4.3.6.22.1 Module Management Inputs

4.3.6.22.1.1 D12 – M'm_TEST_DP

The signal M'm'_TEST_DP is the test request which is now sourced from the string management system as a request to the Module Management system over the CAN Bus interface.

4.3.6.22.1.2 P19 - M'm'_TEST_DP

The signal M'm'_TEST_DP is the internal parameter value used to control the output oscillator M'm'_FO_1Hz.

4.3.6.22.1.3 P23 - M'm'_SAFETY_TIME_DP

The signal M'm'_SAFETY_TIME_DP is the internal parameter value used to monitor the timing of the self-test. This timer is independent from the test request which is triggered from the String Management system.

4.3.6.22.1.4 P22 - M'm'_TRIP_DI_V_1

The signal M'm'_TRIP_DI_V_1 is the internal parameter used to test the hardware monitor and provides the NOT TRIPPED or TRIPPED state.

4.3.6.22.1.5 P25 - M'm'_TRIP_DP

The signal M'm'_TRIP_DP is used to indicate to the String Management system that the hardware monitor has tripped. It can also be used by the 5 kHz monitor to set the TRIPPED state if the self-test is not performed in a timely manner.

4.3.6.22.2 String Management Internal

4.3.6.22.2.1 P20 – M'm'_TEST_DP

The signal M'm'_TEST_DP is the internal parameter value used to control the output oscillator via the CAN Bus interface between the String Management system and the Module Management system.

4.3.6.22.2.2 P21 – M'm'_OK_DI_V

The signal M'm'_OK_DI_V is the internal parameter value used for the PcC_5kHZSelf_Test which has now moved from the Module Management controller to the String Management system to offer independence.

4.3.6.22.3 String Management Outputs

4.3.6.22.3.1 D12 – M'm'_TEST_DP

The signal M'm'_TEST_DP is the test request which is now output from the String Management system as a request to the Module Management system over the CAN Bus interface.

4.3.6.23 Cell Voltage Operating Area – Architecture 5 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.3.6.24. Table 67 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 67: BMS Architecture 5 Element Cross Reference to Diagnostic Coverage Claims

Element	**Diagnostic Coverage Calculation Table Reference in Appendix E5 – BMS – Architecture 5 DC% Claims**
5)A5	Table 153: BMS - Architecture 5 Actuator 5
5)A6	Table 154: BMS - Architecture 5 Actuator 6
5)C5	Table 155: BMS - Architecture 5 Connection 5
5)C6	Refer to 5)C5 as similar techniques used
5)D12	Table 156: BMS - Architecture 5 Data 12 (subset 1) Table 157: BMS - Architecture 5 Data 12 (subset 2)
5)M5	Table 158: BMS - Architecture 5 Measurement 5
5)O3	Table 159: BMS - Architecture 5 Output 3
5)T3	Table 160: BMS - Architecture 5 Transducer 3
5)T4	Table 161: BMS - Architecture 5 Transducer 4

4.3.6.23.1 Element '5)A5'

Additional diagnostics using the PPc_5kHzSelf_Test (4.3.6.9.2) to be monitored by the PCc_5kHzST_Monitor (4.3.6.24.1) allow any delay in the self-test to be monitored. This is allocated to an independent microcontroller with separate time bases so high integrity is achieved.

4.3.6.23.2 Element '5)A6'

Diagnostics are significantly increased by inclusion of the self-test monitor PCc_5kHzST_Monitor (4.3.6.24.1). As the positive and negative contactors are independent, having additional diagnostics devoted to the negative contactor offers improved detection capability.

4.3.6.23.3 Element '5)C5', '5)C6'

As the connections are now monitored by PCc_5kHzSelf_Test (4.3.6.9.2) and, as a secondary measure, checked for timing by PCc_5kHzST_Monitor (4.3.6.24.1) diagnostic coverage is significantly increased.

4.3.6.23.4 Element '5)D12'

Normal CAN diagnostics are applied to this data element.

4.3.6.23.5 Element '5)M5'

As this is part of the closed loop trip signal it is effectively covered by PCc_5kHzSelf_Test.

4.3.6.23.6 Element '5)O3'

As this is part of the closed loop trip signal it is effectively covered by PCc_5kHzSelf_Test.

4.3.6.23.7 Element '5)T3'

Diagnostics are increased by a combination of the PCc6801_Self_Test and the PCc_5kHzSelf_Test now being performed independently in the String Management microcontroller. The combination improves failure detection.

4.3.6.23.8 Element '5)T4'

Increased diagnostics are achieved by the monitoring of the PCc_5kHzSelf_Test in the String Management microcontroller.

4.3.6.24 Cell Voltage Operating Area – Architecture 5 Plausibility Cross-checks

4.3.6.24.1 PCc_5kHzST_Monitor

To ensure that the PCc_5kHzSelf_Test is completed regularly and within a time window tolerance, a separate monitor is included. This monitoring PCc is performed in the Module Management microcontroller which has its own power supply and timing crystal and so is completely independent to the PCc_5kHzSelf_test function which is performed in the String Management microcontroller.

4.3.6.25 Cell Voltage Operating Area – Architecture 5 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 68 and the LFM calculation shown in Table 69.

Table 68: Maintain OA Architecture 5 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Failure mode that has the potential to violate the SG in the absense of a Safety Mechanism	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Connections										
C'c'_AI_0V001	Connection	1)C1	0.6	Y	0.6	45%	Y	PCc_6803_Self_Test	42.00%	0.1566
C'c'_AI_0V	Connection	1)C2	0.05	Y	0.05	45%	Y	PCc_6803_Self_Test	72.00%	0.0063
HW Monitor										
C'c'_AI_0V001	Measurement	2)M3	24	Y	24	45%	Y	PCc_6803_Self_Test	64.83%	3.79836
C'c'_AI_0V001	Transducer	5)T3	25	Y	25	45%	Y	OA Window, PCC 6803 Self Test	97.54%	0.276778125
BATT'b'_PO_PC	Actuator	5)A5	0.5		0	45%		PCc_5kHzSelft_Test	99.00%	
SPI ADC Inputs										
C'c'_AI_0V001	Measurement	2)M1	102	Y	102	45%	Y	PCc_OA_Window, PCc_6803_Self_Test	98.21%	0.819855
SPI ADC Internal										
VMEAS_AI_TX	Transducer	1)T1	50	Y	50	45%	Y	PCc_OA_Window, PCc_6803_Self_Test	97.74%	0.50900625
SPI ADC Outputs										
VMEAS_AI_TX	Data	1)D1	3	Y	3	45%	Y	PCc_Data_Checksum, PCc_Poll_Response_Time	90.79%	0.124308
Module Management Inputs										
VMEAS_AI_TX	Data	1)D2	3	Y	3	45%	Y	PCc_Data_Checksum, PCc_Poll_Response_Time	90.79%	0.124308
M'm'_TRIP_FO_1Hz	Measurement	4)M4	3.5	Y	3.5	45%	Y	PCc_5kHzSelft_Test	44.64%	0.87192
M'm'_TEST_DP	Data	5)D12	3	Y	3	45%	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.053595
Module Management Internals										
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	45%	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test	94.08%	0.119930625
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	45%	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test, CRC on CAL Tables	94.37%	0.113972063
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	45%	Y		98.28%	0.00774
M'm'_TRIP_DI_V	Output	5)O3	25	Y	25	45%	Y	PCc_PSU_Mon	98.26%	0.19603125
Power Supply	General - PSU	1)PSU1	60	Y	60	45%	Y	PCc_PSU_Mon	98.51%	0.40365
Module Management Outputs										
M'm'_OA_TRIP_DP	Data	1)D3	3	Y	3	45%	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.053595
M'm'_TRIP_DO_V	Connection	5)C5	0.05	Y	0.05	45%	Y	PCc_5kHzSelf_Test	99.00%	0.000225
BATT'b'_PO_PC	Output	4)O7	0.5		0	45%		PCc_5kHzSelf_Test	97.52%	
M'm'_TRIP_DP	Data	4)D11	3		0	45%				
HV Measurement Inputs										
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	45%				
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	45%				
HV Measurement Internal										
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	45%				
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%				
S's'_HVPOS_AI_1V,HVPOS_BUS_A	Transducer	1)T2	14		0	45%				
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	45%				
Power Supply	General - PSU	1)PSU2	20		0	45%				
HV Measurement Outputs										
S's'_HVPOS_AI_1V	Data	1)D7	3		0	45%				
String Management Inputs										
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	45%	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.10719
M'm'_TRIP_DO_V	Connection	5)C6	0.05	Y	0.05	45%	Y		0.00%	0.0225
M'm'_TRIP_DP	Data	4)D11	3		0	45%				
String Management Internal										
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	45%	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test	94.08%	0.23986125
SAFETY_OK_DI_V	Measurement	5)M5	4	Y	4	45%	Y	PCc_5kHzSelf_Test	79.82%	0.363222
M'm'_OK_DLY_DI_V	Transducer	5)T4	8	Y	8	45%	Y	PCc_PSU_Mon,PCc_5kHzSelf_Test	80.34%	0.707733
Power Supply	General - PSU	1)PSU3	40	Y	40	45%	Y	PCc_PSU_Mon	98.51%	0.2691
String Management Outputs										
HVPOS1P_DHO_V	Output	1)O1	20	Y	20	45%	Y	PCc_PSU_Mon	0.00%	9
HVNEGN_DLO_V	Output	1)O2	20		0	45%				
M'm'_TEST_DP	Data	5)D12	3	Y	3	45%	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.053595
String Hardware Logic Inputs										
M'm'_OK_DLY_DI_V	Actuator	5)A6	12	Y	12	45%	Y	PCc_PSU_Mon	98.28%	0.09288
String Hardware Logic outputs										
HVPOS1N_DLO_V	Output	2)O5	20	Y	20	45%	Y	PCc_PSU_Mon	0.00%	9
HVNEGP_DHO_V	Output	2)O6	20	Y	20	45%	Y	PCc_PSU_Mon	0.00%	9
Coils										
HVPOS1P_DHO_V	Actuator	1)A1	15	Y	15	100%	Y	PCc_PSU_Mon	0.00%	15
HVPOS1N_DHSO	Actuator	2)A4	15	Y	15	100%	Y	PCc_PSU_Mon	0.00%	15
HVNEGN_DLO_V	Actuator	1)A2	15	Y	15	100%	Y			15
HVNEGP_DHO_V	Actuator	2)A7	15	Y	15	100%	Y	PCc_PSU_Mon	0.00%	15
			597.15		**514.25**		**SPFM =**	**81.2%**		**96.49**

Table 69: Maintain OA Architecture 5 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %		Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Failure Mode coverage with respect to Latent failures, %	Latent multiple-Point failure rate/FIT
Connections													
C'c'_AI_0V001	Connection	1)C1	0.6	Y	0.6	45%	0.1134	Y	100.00%	0.1134	PCc_HW_MONITOR with	72.00%	0.031752
C'c'_AI_0V	Connection	1)C2	0.05	Y	0.05	45%	0.0162	Y	100.00%	0.0162	PCc_HW_MONITOR with	72.00%	0.004536
HW Monitor													
C'c'_AI_0V001	Measurement	2)M3	24	Y	24	45%	7.00164	y	100.00%	7.0016			7.00164
C'c'_AI_0V001	Transducer	5)T3	25	Y	25	45%	10.97322188	y	100.00%	10.9732			10.97322188
BATT'b'_PO_PC	Actuator	5)A5	0.5		0	45%	0	y	100.00%	0.0000			0
SPI ADC Inputs													
C'c'_AI_0V001	Measurement	2)M1	102	Y	102	45%	45.080145	Y	100.00%	45.0801	PCc_HW_MONITOR with	72.00%	12.6224406
SPI ADC Internal													
VMEAS_AI_TX	Transducer	1)T1	50	Y	50	45%	21.99099375	Y	100.00%	21.9910	PCc_HW_MONITOR with	72.00%	6.15747825
SPI ADC Outputs													
VMEAS_AI_TX	Data	1)D1	3	Y	3	45%	1.225692	Y	100.00%	1.2257	PCc_HW_MONITOR with	72.00%	0.34319376
Module Management Inputs													
VMEAS_AI_TX	Data	1)D2	3	Y	3	45%	1.225692	Y	100.00%	1.2257	PCc_HW_MONITOR with	72.00%	0.34319376
M'm'_TRIP_FO_1Hz	Measurement	4)M4	3.5	Y	3.5	45%	0.70308	Y	100.00%	0.7031	Wdog	90.00%	0.070308
M'm'_TEST_DP	Data	5)D12	3	Y	3	45%	1.296405			0.0000			
Module Management Internals													
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	45%	1.905069375	Y	100.00%	1.9051	Wdog	90.00%	0.190506938
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	45%	1.911027938	Y	100.00%	1.9110	Wdog	90.00%	0.191102794
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	45%	0.44226	Y	100.00%	0.4423			0.44226
M'm'_TRIP_DI_V	Output	5)O3	25	Y	25	45%	11.05396875	Y	100.00%	11.0540			11.05396875
Power Supply	General - PSU	1)PSU1	60	Y	60	45%	26.59635	Y	100.00%	26.5964	Wdog	90.00%	2.659635
Module Management Outputs													
M'm'_OA_TRIP_DP	Data	1)D3	3	Y	3	45%	1.296405	Y	100.00%	1.2964	PCc_HW_MONITOR with	72.00%	0.3629934
M'm'_TRIP_DO_V	Connection	5)C5	0.05	Y	0.05	45%	0.022275			0.0000			
BATT'b'_PO_PC	Output	4)O7	0.5		0	45%	0			0.0000			
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
HV Measurement Inputs													
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	45%	0			0.0000			
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	45%	0			0.0000			
HV Measurement Internal													
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	45%	0			0.0000			
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,HVPOS_BUS_A	Transducer	1)T2	14		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	45%	0			0.0000			
Power Supply	General - PSU	1)PSU2	20		0	45%	0			0.0000			
HV Measurement Outputs													
S's'_HVPOS_AI_1V	Data	1)D7	3		0	45%	0			0.0000			
String Management Inputs													
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	45%	2.59281	Y	100.00%	2.5928	PCc_HW_MONITOR with	72.00%	0.7259868
M'm'_TRIP_DO_V	Connection	5)C6	0.05	Y	0.05	45%	0			0.0000			
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
String Management Internal													
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	45%	3.81013875	Y	100.00%	3.8101	Wdog	90.00%	0.381013875
SAFETY_OK_DI_V	Measurement	5)M5	4	Y	4	45%	1.436778	Y	100.00%	1.4368			1.436778
M'm'_OK_DLY_DI_V	Transducer	5)T4	8	Y	8	45%	2.892267	Y	100.00%	2.8923			2.892267
Power Supply	General - PSU	1)PSU3	40	Y	40	45%	17.7309	Y	100.00%	17.7309	Wdog	90.00%	1.77309
String Management Outputs													
HVPOS1P_DHO_V	Output	1)O1	20	Y	20	45%	0	Y	100.00%	0.0000	PCc_HW_MONITOR with	72.00%	0
HVNEGN_DLO_V	Output	1)O2	20		0	45%	0	y	100.00%	0.0000			0
M'm'_TEST_DP	Data	5)D12	3	Y	3	45%	1.296405			0.0000			
String Hardware Logic Inputs													
M'm'_OK_DLY_DI_V	Actuator	5)A6	12	Y	12	45%	5.30712	y	100.00%	5.3071			5.30712
String Hardware Logic outputs													
HVPOS1N_DLO_V	Output	2)O5	20	Y	20	45%	0	y	100.00%	0.0000			0
HVNEGP_DHO_V	Output	2)O6	20	Y	20	45%	0	y	100.00%	0.0000			0
Coils													
HVPOS1P_DHO_V	Actuator	1)A1	15	Y	15	100%	0	Y	100.00%	0.0000	PCc_HW_MONITOR with	72.00%	0
HVPOS1N_DHSO	Actuator	2)A4	15	Y	15	100%	0	y	100.00%	0.0000			0
HVNEGN_DLO_V	Actuator	1)A2	15	Y	15	100%	0	y	100.00%	0.0000			0
HVNEGP_DHO_V	Actuator	2)A7	15	Y	15	100%	0	y	100.00%	0.0000			0
			597.15		**514.25**		**LFM =**	**84.4%**					**64.96**

The independence between the two systems (the module management and string management) has significantly improved the SPFM value from 78% to 81.2% and LFM from 79.8% to 84.4%. The self-test is now independently monitored and the timing of the self-test is also independently monitored.

It is believed that improvements in the diagnostic coverage of the low voltage measurement system will be difficult to obtain. However, there is still no coverage on the high voltage measurement and there is an obvious route to validate this against the sum of the individual cell voltages as discussed in architecture 6.

4.3.6.26 Cell Voltage Operating Area – Architecture 6

Building on Architecture 5, Architecture 6 (Figure 28) adds an additional cross check (PCc HVPOSBATT) between the high voltage measurements and the cell voltage measurements.

This allows verification between the voltage measured across the string (summation of the module voltages internal to the string contactors) and that measured across the load on the output side of the contactors. The module voltages are in turn the sum of the individual cell voltages.

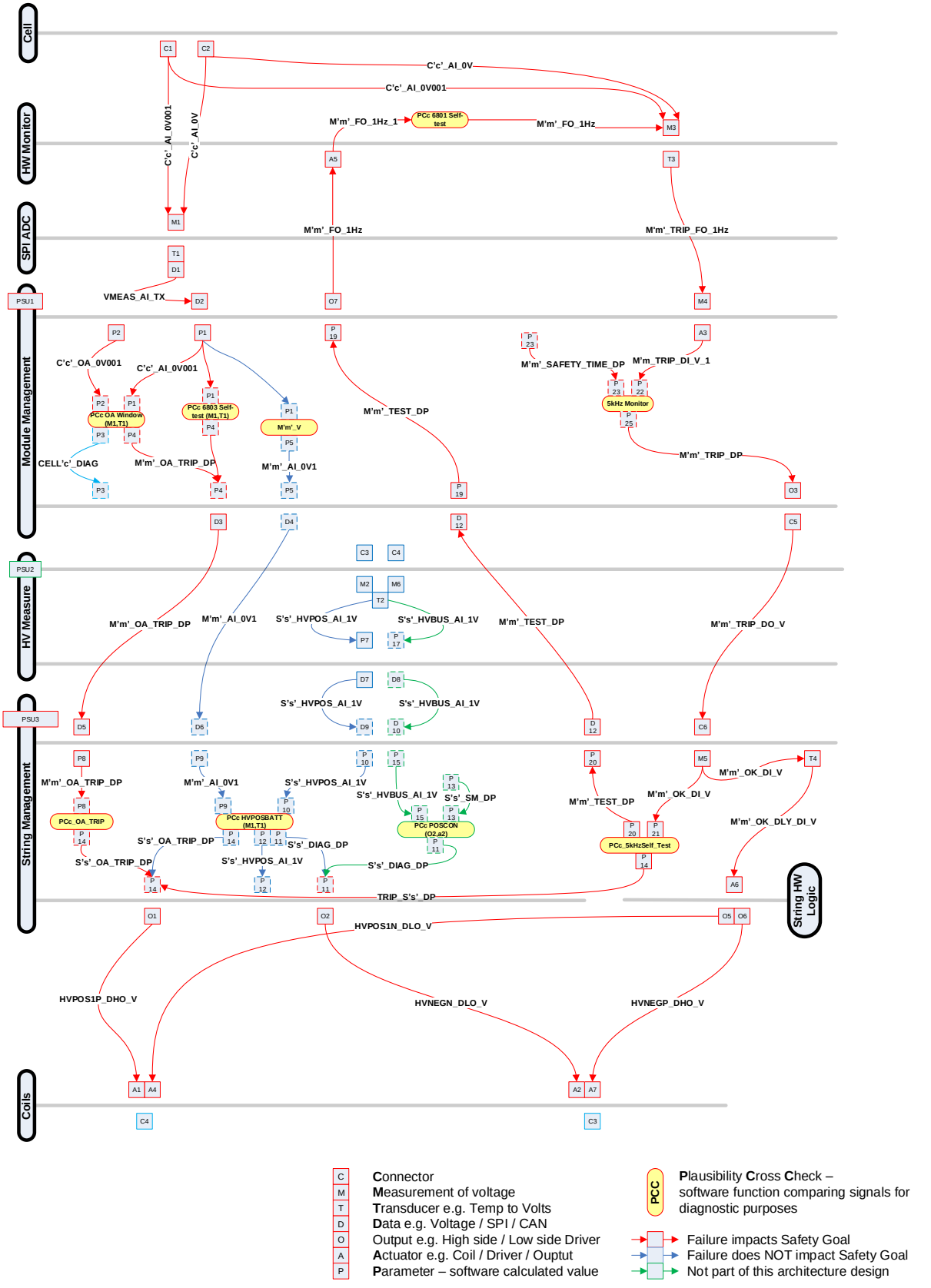


Figure 28: Maintain OA - Concept Architecture Candidate 6

4.3.6.27 Cell Voltage Operating Area – Architecture 6 Classified Signals

Any new signals or signals with increased diagnostic coverage are detailed in this section.

4.3.6.27.1 Module Management Internals

4.3.6.27.1.1 P5 - M'm'_AI_0V1

The signal M'm'_AI_0V1 is the module voltage with a resolution of 0.1V. It is calculated based on the sum of voltages equation (see equation 19) from each of the individual cells (C'c'_AI_0V001) in the module.

$$\boldsymbol{M'm'\_AI\_0V1} = \sum_{'c'=1}^{'c'=12} \boldsymbol{C'c'\_AI\_0V001} \quad (19)$$

Where 'c' is the number of cells and the maximum (12) for the LTC6803 is used in this example.

4.3.6.27.2 Module Management Outputs

4.3.6.27.2.1 D4 - M'm'_AI_0V1

The signal M'm'_AI_0V1 transmitted from the Module Management CAN Bus interface.

4.3.6.27.2.2 D11 - M'm'_TRIP_DP

The signal M'm'_TRIP_DP transmitted from the Module Management CAN Bus interface.

4.3.6.27.2.3 C5 - M'm'_TRIP_DI_V_1

The hard-wired output from the module management that indicates to the String Management that the hardware monitor has tripped.

4.3.6.27.3 HV Measurement Inputs

4.3.6.27.3.1 C3 - S's'_HVPOS_AI_1V

S's'_HVPOS_AI_1V is the high voltage positive voltage at the output of the contactor. This allows voltages to be measured before and after contactor opening / closuring. It is purely used for diagnostics as far as functional safety is concerned.

4.3.6.27.3.2 C4 - S's'_HVBUS_AI_1V

S's'_HVBUS_AI_1V is the positive high voltage at the output of the battery (before the contactor). This allows voltages to be measured before either of the contactors have been closed and after

either contactor has been closed. It is purely used for diagnostics as far as functional safety is concerned.

4.3.6.27.4 HV Measurement Internal

4.3.6.27.4.1 PSU2 - Power Supply

The internal power supply for the HV Measurement system and any other voltages required by the measurement system, this would typically include isolated power supplies (DC-DC converters) to isolate the HV from the LV (chassis referenced systems) and the local microcontroller supplies along with analogue references etc.

4.3.6.27.4.2 M2 - S's'_HVPOS_AI_1V

The voltage measurement for S's'_HVPOS_AI_1V.

4.3.6.27.4.3 M6 - S's'_HVBUS_AI_1V

The voltage measurement for S's'_HVBUS_AI_1V.

4.3.6.27.4.4 T2 - S's'_HVPOS_AI_1V

The conversion mechanism for S's'_HVPOS_AI_1V is classed as a transducer due to the scaling involved to convert the high voltage to low voltage for use in the analogue to digital converters and the isolation required between high and low voltage as the low voltage is referenced to the chassis of the vehicle but the high voltage is isolated.

4.3.6.27.4.5 T2 - S's'_HVBUS_AI_1V

The conversion mechanism for S's'_HVBUS_AI_1V is classed as a transducer due to the scaling and isolation involved. The transducer is classed as shared between S's'_HVPOS_AI_V and S's'_HVBUS_AI_V.

4.3.6.27.4.6 P7 - S's'_HVPOS_AI_1V

The internal parameter for S's'_HVPOS_AI_1V as a scaled voltage value with a resolution of 1V.

4.3.6.27.5 HV Measurement Outputs

4.3.6.27.5.1 D7 - S's'_HVPOS_AI_1V

S's'_HVPOS_AI_1V transmitted data on the CAN Bus interface.

4.3.6.27.6 String Management Inputs

4.3.6.27.6.1 D6 - M'm'_AI_0V1

The signal M'm'_AI_0V1 received at the String Management CAN bus interface.

4.3.6.27.6.2 D9 - S's'_HVPOS_AI_1V

S's'_HVPOS_AI_1V received at the String Management CAN bus interface.

4.3.6.27.7 String Management Internal

4.3.6.27.7.1 P9 – M'm'_AI_0V1

The internal parameter M'm'_AI_0V1 used by the String Management application.

4.3.6.27.7.2 P10 – S's_HVPOS_AI_1V

The internal value S's'_HVPOS_AI_1V used by the String Management application.

4.3.6.27.7.3 P12 – S's'_HVPOS_AI_1V

An internal value used in the String Management system. This is also likely to be transmitted onto the CAN bus for diagnostic purposes and is not considered further as part of the safety critical analysis.

4.3.6.27.7.4 P11 – S's'_DIAG_DP

If the plausibility check PCc_HVPOSBATT (4.3.6.29.1) detects failures then the S's'_Diag_DP flag is set which can provide a redundant path to open the contactors via O2 – HVPOS1N_DLO_V.

4.3.6.27.8 String Management Outputs

4.3.6.27.8.1 O2 - HVNEGN_DLO_V

The low side drive of the high voltage negative contactor.

4.3.6.27.9 Coils

4.3.6.27.9.1 A2 - HVNEGN_DLO_V

The negative side of the high voltage negative contactor coil.

4.3.6.28 Cell Voltage Operating Area – Architecture 6 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.3.6.29. Table 70 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 70: BMS Architecture 6 Element Cross Reference to Diagnostic Coverage Claims

Element	Diagnostic Coverage Calculation Table Reference in Appendix E7 – BMS – Architecture 7 DC% Claims
6)A1	Table 162: BMS - Architecture 6 Actuator 1
6)A2	Refer to 6)A1 as similar techniques used
6)A4	Refer to 6)A1 as similar techniques used
6)A7	Refer to 6)A1 as similar techniques used
6)C1	Table 163: BMS - Architecture 6 Connection 1
6)C2	Refer to 6)C1 as similar techniques used
6)M1	Table 164: BMS - Architecture 6 Measurement 1
6)M3	Table 165: BMS - Architecture 6 Measurement 3
6)O1	Table 166: BMS - Architecture 6 Output 1
6)O2	Refer to 6)O1 as similar techniques used
6)O5	Refer to 6)O1 as similar techniques used
6)O6	Refer to 6)O1 as similar techniques used
6)T1	Table 167: BMS - Architecture 6 Transducer 1
6)T3	Table 168: BMS - Architecture 6 Transducer 3

4.3.6.28.1 Element '6)A1', '6)A2', '6)A4', '6)A7'

Diagnostics are now significantly increased due to the ability to monitor the contactors before and after operation.

4.3.6.28.2 Element '6)C1'

PCc_HVPosBatt also allows additional diagnostics on the Cell measurement side. Although the HV measurement is not as accurate as the AFE cell measurement it can still provide suitable diagnostics.

4.3.6.28.3 Element '6)C2'

Identical argument to '6)C1' (4.3.6.28.2).

4.3.6.28.4 Element '6)M1'

A combination of PCcs are now used to diagnose appropriate failure modes in the measurement side of the AFE. This combination gives a higher confidence level in the PCc.

4.3.6.28.5 Element '6)M3'

Again, a combination of PCcs allows an increase in confidence that the hardware monitor is working correctly.

4.3.6.28.6 Element '6)O1', '6)O2', '6)O5', '6)O6'

As this output is directly connected to the contactor and feedback is available from the contactor output, diagnostics are increased.

4.3.6.28.7 Element '6)T1', '6)T3'

A combination of the PCcs now allows changes to be monitored i.e. increases or decreases in cell voltages will be reflected in changes at the Battery HV measurement. Slight delays may occur due to the independent measurement systems but averaging and a time window will adequately compensate for this and overall, contribute to a high level of diagnostic coverage.

4.3.6.29 Cell Voltage Operating Area – Architecture 6 Plausibility Cross-checks

4.3.6.29.1 PCc_HVPOSBATT

This PCc is specific to the application (rather than the more generic PCcs discussed earlier for the Cell Management system). A measurement is made of the HV battery voltage once the negative contactor has been closed. It permits a PCc against the sum of the individual module voltages, which are in turn calculated from the sum of the individual block voltages. As this is a high voltage measurement, the accuracy is likely to be reduced. The measurement is of sufficient integrity to validate the sum of the module voltages and the string voltage prior to closing the positive contactor and applying string voltage to the Bus. By careful sequencing of this test, several failure modes can be detected.

4.3.6.30 Cell Voltage Operating Area – Architecture 6 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 71 and the LFM calculation shown in Table 72.

Table 71: Maintain OA Architecture 6 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %		Failure mode that has the potential to violate the SG in the absense of a Safety Mechanism	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Connections											
C'c'_AI_0V001	Connection	6)C1	0.6	Y	0.6	40%	0.2400	Y	PCc_6803_Self_Test, PCc_HVPosBatt	99.00%	0.0024
C'c'_AI_0V	Connection	6)C2	0.05	Y	0.05	40%	0.0200	Y	PCc_6803_Self_Test, PCc_HVPosBatt	99.00%	0.0002
HW Monitor											
C'c'_AI_0V001	Measurement	6)M3	24	Y	24	40%	9.6000	Y	PCc_6803_Self_Test, PCc_HVPosBatt	98.58%	0.136392
C'c'_AI_0V001	Transducer	6)T3	25	Y	25	40%	10.0000	Y	OA Window, PCC 6803 Self Test, PCc_HVPosBat	98.18%	0.181675
BATT'b'_PO_PC	Actuator	5)A5	0.5	Y	0.5	40%	0.2000	Y	PCc_5kHzSelft_Test	99.00%	0.002
SPI ADC Inputs											
C'c'_AI_0V001	Measurement	6)M1	102	Y	102	40%	40.8000	Y	PCc_OA_Window, PCc_6803_Self_Test, PCc_HVPosBatt	98.58%	0.579666
SPI ADC Internal											
VMEAS_AI_TX	Transducer	6)T1	50	Y	50	40%	20.0000	Y	PCc_OA_Window, PCc_6803_Self_Test	97.94%	0.41285
SPI ADC Outputs											
VMEAS_AI_TX	Data	1)D1	3	Y	3	40%	1.2000	Y	PCc_Data_Checksum, PCc_Poll_Response_Time	90.79%	0.110496
Module Management Inputs											
VMEAS_AI_TX	Data	1)D2	3	Y	3	40%	1.2000	Y	PCc_Data_Checksum, PCc_Poll_Response_Time	90.79%	0.110496
M'm'_TRIP_FO_1Hz	Measurement	4)M4	3.5	Y	3.5	40%	1.4000	Y	PCc_5kHzSelft_Test	44.64%	0.77504
M'm'_TEST_DP	Data	5)D12	3	Y	3	40%	1.2000	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.04764
Module Management Internals											
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	40%	1.8000	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test	94.08%	0.106605
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	40%	1.8000	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test, CRC on CAL Tables	94.37%	0.1013085
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	40%	0.4000	Y		98.28%	0.00688
M'm'_TRIP_DI_V	Output	5)O3	25	Y	25	40%	10.0000	Y	PCc_PSU_Mon	98.26%	0.17425
Power Supply	General - PSU	1)PSU1	60	Y	60	40%	24.0000	Y	PCc_PSU_Mon	98.51%	0.3588
Module Management Outputs											
M'm'_OA_TRIP_DP	Data	1)D3	3	Y	3	40%	1.2000	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.04764
M'm'_TRIP_DO_V	Connection	5)C5	0.05	Y	0.05	40%	0.0200	Y	PCc_5kHzSelf_Test	99.00%	0.0002
BATT'b'_PO_PC	Output	4)O7	0.5	Y	0.5	40%	0.2000	Y	PCc_5kHzSelf_Test	97.52%	0.00497
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0.0000				
HV Measurement Inputs											
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	40%	0.0000				
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	40%	0.0000				
HV Measurement Internal											
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	40%	0.0000				
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0.0000				
S's'_HVPOS_AI_1V,HVPOS_BUS_A	Transducer	1)T2	14		0	40%	0.0000				
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	40%	0.0000				
Power Supply	General - PSU	1)PSU2	20		0	40%	0.0000				
HV Measurement Outputs											
S's'_HVPOS_AI_1V	Data	1)D7	3		0	40%	0.0000				
String Management Inputs											
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	40%	2.4000	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.09528
M'm'_TRIP_DO_V	Connection	5)C6	0.05	Y	0.05	40%	0.0200	Y	PCc_5kHzSelf_Test	99.00%	0.0002
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0.0000				
String Management Internal											
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	40%	3.6000	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test	94.08%	0.21321
SAFETY_OK_DI_V	Measurement	5)M5	4	Y	4	40%	1.6000	Y	PCc_5kHzSelf_Test	79.82%	0.322864
M'm'_OK_DLY_DI_V	Transducer	5)T4	8	Y	8	40%	3.2000	Y	PCc_PSU_Mon,PCc_5kHzSelf_Test	80.34%	0.629096
Power Supply	General - PSU	1)PSU3	40	Y	40	40%	16.0000	Y	PCc_PSU_Mon	98.51%	0.2392
String Management Outputs											
HVPOS1P_DHO_V	Output	1)O1	20	Y	20	45%	9.0000	Y	PCc_PSU_Mon	0.00%	9
HVNEGN_DLO_V	Output	1)O2	20		0	45%	0.0000				
M'm'_TEST_DP	Data	5)D12	3	Y	3	45%	1.3500	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.053595
String Hardware Logic Inputs											
M'm'_OK_DLY_DI_V	Actuator	5)A6	12	Y	12	40%	4.8000	Y	PCc_PSU_Mon, PCc_HVPOSBAT	98.28%	0.08256
String Hardware Logic outputs											
HVPOS1N_DLO_V	Output	2)O5	20	Y	20	45%	9.0000	Y	PCc_PSU_Mon	0.00%	9
HVNEGP_DHO_V	Output	2)O6	20	Y	20	45%	9.0000	Y	PCc_PSU_Mon	0.00%	9
Coils											
HVPOS1P_DHO_V	Actuator	1)A1	15	Y	15	100%	15.0000	Y	PCc_PSU_Mon	0.00%	15
HVPOS1N_DHSO	Actuator	2)A4	15	Y	15	100%	15.0000	Y	PCc_PSU_Mon	0.00%	15
HVNEGN_DLO_V	Actuator	1)A2	15	Y	15	100%	15.0000	Y			15
HVNEGP_DHO_V	Actuator	2)A7	15	Y	15	100%	15.0000	Y	PCc_PSU_Mon	0.00%	15
			597.15		**515.25**			**SPFM =**	**82.2%**		**91.80**

Table 72: Maintain OA Architecture 6 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %		Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Failure Mode coverage with respect to Latent failures, %	Latent.multiple-Point failure rate/FIT
Connections													
C'c'_AI_0V001	Connection	6)C1	0.6	Y	0.6	40%	0.2376	Y	100.00%	0.2376	PCc_HW_MONITOR with	72.00%	0.066528
C'c'_AI_0V	Connection	6)C2	0.05	Y	0.05	40%	0.0198	Y	100.00%	0.0198	PCc_HW_MONITOR with	72.00%	0.005544
HW Monitor													
C'c'_AI_0V001	Measurement	6)M3	24	Y	24	40%	9.463608	y	100.00%	9.4636	PCc_HVPOSBATT	40.00%	5.6781648
C'c'_AI_0V001	Transducer	6)T3	25	Y	25	40%	9.818325	y	100.00%	9.8183	PCc_HVPOSBATT	40.00%	5.890995
BATT'b'_PO_PC	Actuator	5)A5	0.5	Y	0.5	40%	0.198	y	100.00%	0.1980	PCc_HVPOSBATT	40.00%	0.1188
SPI ADC Inputs													
C'c'_AI_0V001	Measurement	6)M1	102	Y	102	40%	40.220334	Y	100.00%	40.2203	PCc_HW_MONITOR with	72.00%	11.26169352
SPI ADC Internal													
VMEAS_AI_TX	Transducer	6)T1	50	Y	50	40%	19.58715	Y	100.00%	19.5872	PCc_HW_MONITOR with	72.00%	5.484402
SPI ADC Outputs													
VMEAS_AI_TX	Data	1)D1	3	Y	3	40%	1.089504	Y	100.00%	1.0895	PCc_HW_MONITOR with	72.00%	0.30506112
Module Management Inputs													
VMEAS_AI_TX	Data	1)D2	3	Y	3	40%	1.089504	Y	100.00%	1.0895	PCc_HW_MONITOR with	72.00%	0.30506112
M'm'_TRIP_FO_1Hz	Measurement	4)M4	3.5	Y	3.5	40%	0.62496	Y	100.00%	0.6250	Wdog	90.00%	0.062496
M'm'_TEST_DP	Data	5)D12	3	Y	3	40%	1.15236			0.0000			
Module Management Internals													
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	40%	1.693395	Y	100.00%	1.6934	Wdog	90.00%	0.1693395
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	40%	1.6986915	Y	100.00%	1.6987	Wdog	90.00%	0.16986915
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	40%	0.39312	Y	100.00%	0.3931			0.39312
M'm'_TRIP_DI_V	Output	5)O3	25	Y	25	40%	9.82575	Y	100.00%	9.8258			9.82575
Power Supply	General - PSU	1)PSU1	60	Y	60	40%	23.6412	Y	100.00%	23.6412	Wdog	90.00%	2.36412
Module Management Outputs													
M'm'_OA_TRIP_DP	Data	1)D3	3	Y	3	40%	1.15236	Y	100.00%	1.1524	PCc_HW_MONITOR with	72.00%	0.3226608
M'm'_TRIP_DO_V	Connection	5)C5	0.05	Y	0.05	40%	0.0198			0.0000			
BATT'b'_PO_PC	Output	4)O7	0.5	Y	0.5	40%	0.19503			0.0000			
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
HV Measurement Inputs													
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	40%	0			0.0000			
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	40%	0			0.0000			
HV Measurement Internal													
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	40%	0			0.0000			
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,HVPOS_BUS_A	Transducer	1)T2	14		0	40%	0			0.0000			
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	40%	0			0.0000			
Power Supply	General - PSU	1)PSU2	20		0	40%	0			0.0000			
HV Measurement Outputs													
S's'_HVPOS_AI_1V	Data	1)D7	3		0	40%	0			0.0000			
String Management Inputs													
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	40%	2.30472	Y	100.00%	2.3047	PCc_HW_MONITOR with	72.00%	0.6453216
M'm'_TRIP_DO_V	Connection	5)C6	0.05	Y	0.05	40%	0.0198			0.0000			
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
String Management Internal													
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	40%	3.38679	Y	100.00%	3.3868	Wdog	90.00%	0.338679
SAFETY_OK_DI_V	Measurement	5)M5	4	Y	4	40%	1.277136	Y	100.00%	1.2771			1.277136
M'm'_OK_DLY_DI_V	Transducer	5)T4	8	Y	8	40%	2.570904	Y	100.00%	2.5709			2.570904
Power Supply	General - PSU	1)PSU3	40	Y	40	40%	15.7608	Y	100.00%	15.7608	Wdog	90.00%	1.57608
String Management Outputs													
HVPOS1P_DHO_V	Output	1)O1	20	Y	20	45%	0	Y	100.00%	0.0000	PCc_HW_MONITOR with	72.00%	0
HVNEGN_DLO_V	Output	1)O2	20		0	45%	0	y	100.00%	0.0000			0
M'm'_TEST_DP	Data	5)D12	3	Y	3	45%	1.296405			0.0000			
String Hardware Logic Inputs													
M'm'_OK_DLY_DI_V	Actuator	5)A6	12	Y	12	40%	4.71744	y	100.00%	4.7174			4.71744
String Hardware Logic outputs													
HVPOS1N_DLO_V	Output	2)O5	20	Y	20	45%	0	y	100.00%	0.0000			0
HVNEGP_DHO_V	Output	2)O6	20	Y	20	45%	0	y	100.00%	0.0000			0
Coils													
HVPOS1P_DHO_V	Actuator	1)A1	15	Y	15	100%	0	Y	100.00%	0.0000	PCc_HW_MONITOR with	72.00%	0
HVPOS1N_DHSO	Actuator	2)A4	15	Y	15	100%	0	y	100.00%	0.0000			0
HVNEGN_DLO_V	Actuator	1)A2	15	Y	15	100%	0	y	100.00%	0.0000			0
HVNEGP_DHO_V	Actuator	2)A7	15	Y	15	100%	0	y	100.00%	0.0000			0
			597.15		**515.25**		**LFM =**	**87.4%**					**53.55**

Increases in SPFM are minimal but the LFM increase is significant (81.6% to 87.4%) as there are no longer dormant faults in the HV measurement system. The main limitation now is on the outputs from the system i.e. the HV connection from the battery pack to the High Voltage bus on the vehicle. No diagnostic coverage is provided on the contactor outputs from the system meaning that the intent to shut down the system is of high integrity but the final output channels may fail to shut down the system in a safe way. This deficiency is reviewed and analysed in the next architecture.

4.3.6.31 Cell Voltage Operating Area – Architecture 7

In architecture 7 (Figure 29) PCc POSCON is included to check the state of the contactor. This allows a number of tests to be performed based on the status of the string state machine (STR's'_SM). For example, if a cell has exceeded its voltage operating area, the sting state machine will trip and open the positive contactor. PCc _POSCON is then used to verify that the contactor has opened which will prevent further discharge to the load or charge from the charger. If this fails, additional measures can be taken, such as, opening the negative contactor giving an additional redundant safety action.

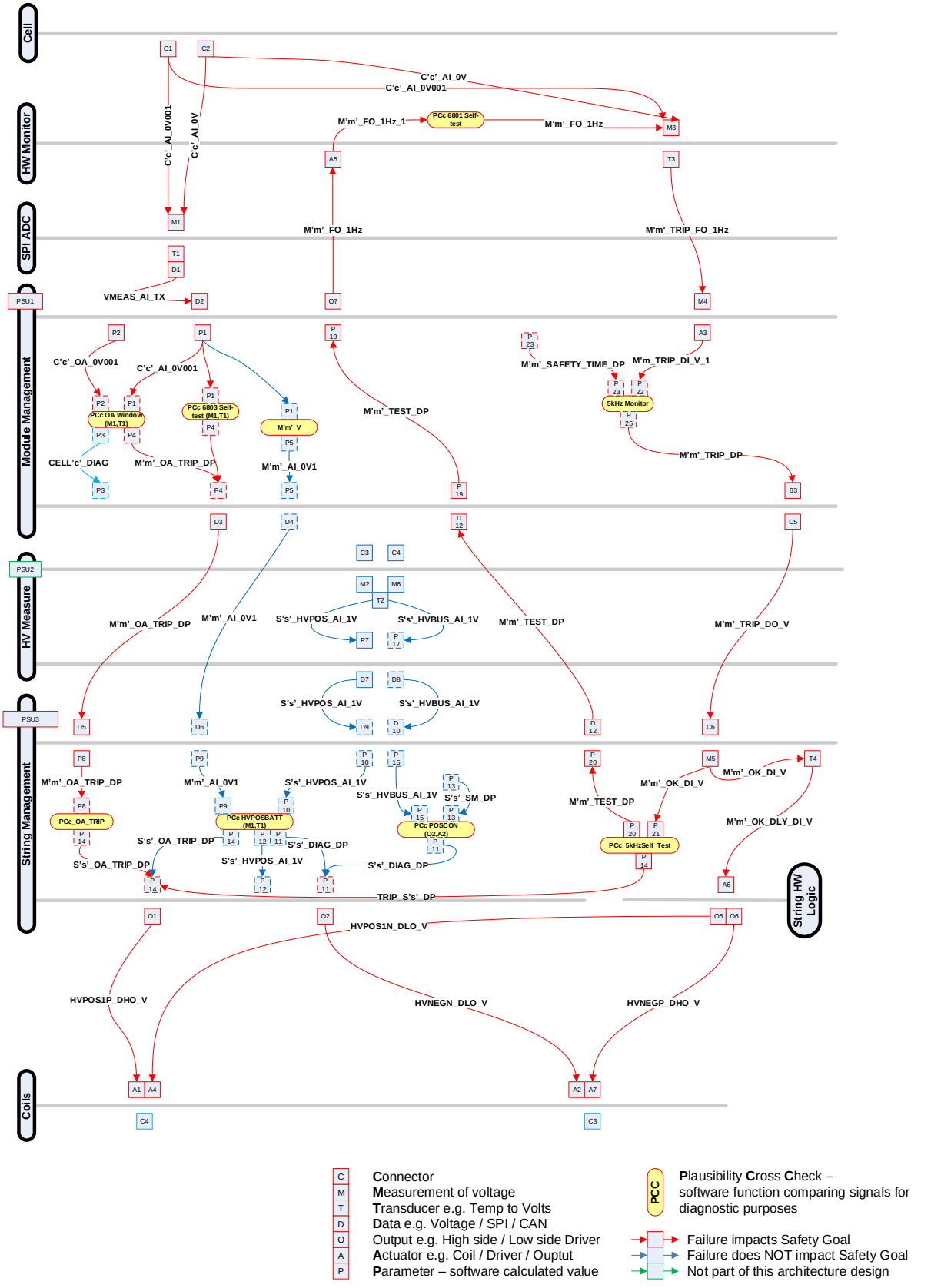


Figure 29: Maintain OA - Concept Architecture Candidate 7

4.3.6.32 Cell Voltage Operating Area – Architecture 7 Classified Signals

New signals and those with increased diagnostic coverage are discussed below.

4.3.6.32.1 HV Measurement Internal

4.3.6.32.1.1 T2 - S's'_HVBUS_AI_1V

The conversion mechanism for S's'_HVBUS_AI_1V is classed as a transducer due to the scaling and isolation involved. The transducer is classed as shared between S's'_HVPOS_AI_V and S's'_HVBUS_AI_V.

4.3.6.32.1.2 P17 - S's'_HVBUS_AI_1V

The internal parameter for S's'_HVBUS_AI_1V as a scaled voltage value with a resolution of 1V.

4.3.6.32.2 HV Measurement Outputs

4.3.6.32.2.1 D8 - S's'_HVBUS_AI_1V

S's'_HVBUS_AI_1V is transmitted data on the CAN Bus interface.

4.3.6.32.3 String Management Inputs

4.3.6.32.3.1 D10 - S's'_HVBUS_AI_1V

S's'_HVBUS_AI_1V received at the String Management CAN bus interface.

4.3.6.32.4 String Management Internal

4.3.6.32.4.1 P15 – S's'_HVBUS_AI_1V

The internal value S's'_HVBUS_AI_1V used by the String Management application.

4.3.6.32.4.2 P13 – S's'_SM_DP

S's'_SM_DP is an internal value that represents the enumerated current state of the String Management system. This is determined by the application and used for all of the main control sequencing between the String Management and Module Management system state machines (SM).

4.3.6.33 Cell Voltage Operating Area – Architecture 7 Diagnostic Coverage

Each of the elements used are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.3.6.34. Table 73 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 73: BMS Architecture 7 Element Cross Reference to Diagnostic Coverage Claims

Element	Diagnostic Coverage Calculation Table Reference in Appendix E5 – BMS – Architecture 5 DC% Claims
7)A1	Table 169: BMS - Architecture 7 Actuator 1
7)A2	Refer to 7)A1 as similar techniques used
7)A4	Refer to 7)A1 as similar techniques used
7)A7	Refer to 7)A1 as similar techniques used
7)O1	Table 170: BMS - Architecture 7 Output 1
7)O2	Refer to 7)O1 as similar techniques used
7)O5	Refer to 7)O1 as similar techniques used
7)O6	Refer to 7)O1 as similar techniques used

4.3.6.33.1 Element '7)A1', '7)A1', '7)A4', '1)A7'

There is no change in the analysis for this actuator. The increase in the PCc claim is achieved by a better definition of the failure modes and the complexity of the actuator and output. At this stage it has been decided to use a simple contactor without any low power modes (economisers) and so all failure modes are identified. This removed the proportion of failures that may require further detailed analysis which gives a slightly higher PCc claim.

4.3.6.33.2 Element '7)O1', '7)O2', '7)O5', '7)O6'

PCc_POSCON is now used to check the output voltages as the contactors are sequenced through their connection and disconnection phases. This gives a higher confidence level that all faults are now detected to (98.5%).

4.3.6.34 Cell Voltage Operating Area – Architecture 7 Plausibility Cross-checks

4.3.6.34.1.1 PCc_POSCON

The bus voltage (STR's'_BUS_AI_V) is measured once both of the contactors are energised (HVNEG is energised AND HVPOS1 energised). STR's'_BUS_AI_V is measured between HVNEG_BUS_AI_V and HVPOS1_BUS_AI_V, this is an independent measurement to the cell voltages and module voltages. As the measurement is outside of the Battery Management System (BMS) it may be necessary to have additional electronics to ensure that there is no leakage path from the inside of the String / Pack to the outside world. This may be as simple as a reed relay controlled by the microcontroller (as used in the initial detailed design).

By enabling the contactors in a specific sequence, contactor faults can be detected on both the positive and negative side. This can also be used as a preventative technique to ensure that

contactors are not closed if the battery voltage is significantly different to the HV BUS. This is not considered a safety issue but more of method to prolong contactor life. It can also aid workshop maintenance when diagnosing reported problems with the systems.

4.3.6.35 Cell Voltage Operating Area – Architecture 7 Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 74 and the LFM calculation shown in Table 75.

Table 74: Maintain OA Architecture 7 SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %		Failure mode that has the potential to violate the SG in the absense of a Safety Mechanism	Safety mechanisms allowing to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Connections											
C'c'_AI_0V001	Connection	6)C1	0.6	Y	0.6	40%	0.2400	Y	PCc_6803_Self_Test, PCc_HVPosBatt	99.00%	0.0024
C'c'_AI_0V	Connection	6)C2	0.05	Y	0.05	40%	0.0200	Y	PCc_6803_Self_Test, PCc_HVPosBatt	99.00%	0.0002
HW Monitor											
C'c'_AI_0V001	Measurement	6)M3	24	Y	24	40%	9.6000	Y	PCc_6803_Self_Test, PCc_HVPosBatt	98.58%	0.136392
C'c'_AI_0V001	Transducer	6)T3	25	Y	25	40%	10.0000	Y	OA Window, PCC 6803 Self Test, PCc_HVPosBat	98.18%	0.181675
BATT'b'_PO_PC	Actuator	5)A5	0.5		0	40%	0.0000		PCc_5kHzSelft_Test	99.00%	
SPI ADC Inputs											
C'c'_AI_0V001	Measurement	6)M1	102	Y	102	40%	40.8000	Y	PCc_OA_Window, PCc_6803_Self_Test, PCc_HVPosBatt	98.58%	0.579666
SPI ADC Internal											
VMEAS_AI_TX	Transducer	6)T1	50	Y	50	40%	20.0000	Y	PCc_OA_Window, PCc_6803_Self_Test	97.94%	0.41285
SPI ADC Outputs											
VMEAS_AI_TX	Data	1)D1	3	Y	3	40%	1.2000	Y	PCc_Data_Checksum, PCc_Poll_Response_Time	90.79%	0.110496
Module Management Inputs											
VMEAS_AI_TX	Data	1)D2	3	Y	3	40%	1.2000	Y	PCc_Data_Checksum, PCc_Poll_Response_Time	90.79%	0.110496
M'm'_TRIP_FO_1Hz	Measurement	4)M4	3.5	Y	3.5	40%	1.4000	Y	PCc_5kHzSelft_Test	44.64%	0.77504
M'm'_TEST_DP	Data	5)D12	3	Y	3	40%	1.2000	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.04764
Module Management Internals											
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	40%	1.8000	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test	94.08%	0.106605
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	40%	1.8000	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test, CRC on CAL Tables	94.37%	0.1013085
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	40%	0.4000	Y		98.28%	0.00688
M'm'_TRIP_DI_V	Output	5)O3	25	Y	25	40%	10.0000	Y	PCc_PSU_Mon	98.26%	0.17425
Power Supply	General - PSU	1)PSU1	60	Y	60	40%	24.0000	Y	PCc_PSU_Mon	98.51%	0.3588
Module Management Outputs											
M'm'_OA_TRIP_DP	Data	1)D3	3	Y	3	40%	1.2000	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.04764
M'm'_TRIP_DO_V	Connection	5)C5	0.05	Y	0.05	40%	0.0200	Y	PCc_5kHzSelf_Test	99.00%	0.0002
BATT'b'_PO_PC	Output	4)O7	0.5	N	0	40%	0.0000		PCc_5kHzSelf_Test	97.52%	
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0.0000				
HV Measurement Inputs											
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	40%	0.0000				
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	40%	0.0000				
HV Measurement Internal											
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	40%	0.0000				
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0.0000				
S's'_HVPOS_AI_1V,HVPOS_BUS_A	Transducer	1)T2	14		0	40%	0.0000				
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	40%	0.0000				
Power Supply	General - PSU	1)PSU2	20		0	40%	0.0000				
HV Measurement Outputs											
S's'_HVPOS_AI_1V	Data	1)D7	3		0	40%	0.0000				
String Management Inputs											
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	40%	2.4000	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.09528
M'm'_TRIP_DO_V	Connection	5)C6	0.05	Y	0.05	40%	0.0200	Y	PCc_5kHzSelf_Test	99.00%	0.0002
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0.0000				
String Management Internal											
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	40%	3.6000	Y	Program sequence in state machines , Scheduled RAM test, Scheduled SW self test	94.08%	0.21321
SAFETY_OK_DI_V	Measurement	5)M5	4	Y	4	40%	1.6000	Y	PCc_5kHzSelf_Test	79.82%	0.322864
M'm'_OK_DLY_DI_V	Transducer	5)T4	8	Y	8	40%	3.2000	Y	PCc_PSU_Mon,PCc_5kHzSelf_Test	80.34%	0.629096
Power Supply	General - PSU	1)PSU3	40	Y	40	40%	16.0000	Y	PCc_PSU_Mon	98.51%	0.2392
String Management Outputs											
HVPOS1P_DHO_V	Output	7)O1	20	Y	20	40%	8.0000	Y	PCc_PSU_Mon, PCc_POSCON	98.51%	0.1196
HVNEGN_DLO_V	Output	7)O2	20	Y	20	40%	8.0000	Y	PCc_PSU_Mon, PCc_POSCON	98.51%	0.1196
M'm'_TEST_DP	Data	5)D12	3	Y	3	45%	1.3500	Y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time	96.03%	0.053595
String Hardware Logic Inputs											
M'm'_OK_DLY_DI_V	Actuator	6)A6	12	Y	12	40%	4.8000	Y	PCc_PSU_Mon	98.28%	0.08256
String Hardware Logic outputs											
HVPOS1N_DLO_V	Output	7)O5	20	Y	20	40%	8.0000	Y	PCc_PSU_Mon, PCc_POSCON	98.51%	0.1196
HVNEGP_DHO_V	Output	7)O6	20	Y	20	40%	8.0000	Y	PCc_PSU_Mon, PCc_POSCON	98.51%	0.1196
Coils											
HVPOS1P_DHO_V	Actuator	7)A1	15	y	15	100%	15.0000	Y	PCc_PSU_Mon, PCc_HVPosBatt	84.86%	2.27175
HVPOS1N_DHSO	Actuator	7)A4	15	y	15	100%	15.0000	Y	PCc_PSU_Mon, PCc_HVPosBatt	84.86%	2.27175
HVNEGN_DLO_V	Actuator	7)A2	15	y	15	100%	15.0000	Y	PCc_PSU_Mon, PCc_HVPosBatt	84.86%	2.27175
HVNEGP_DHO_V	Actuator	7)A7	15	y	15	100%	15.0000	Y	PCc_PSU_Mon, PCc_HVPosBatt	84.86%	2.27175
			597.15		**534.25**			**SPFM =**	**97.3%**		**14.35**

Table 75: Maintain OA Architecture 7 LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %		Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Failure Mode coverage with respect to Latent failures, %	Latent.multiple-Point failure rate/FIT
Connections													
C'c'_AI_0V001	Connection	6)C1	0.6	Y	0.6	40%	0.2376	Y	100.00%	0.2376	PCc_HW_MONITOR with PCc6	72.00%	0.066528
C'c'_AI_0V	Connection	6)C2	0.05	Y	0.05	40%	0.0198	Y	100.00%	0.0198	PCc_HW_MONITOR with PCc6	72.00%	0.005544
HW Monitor													
C'c'_AI_0V001	Measurement	6)M3	24	Y	24	40%	9.463608	y	100.00%	9.4636	PCc_HVPOSBATT	80.00%	1.8927216
C'c'_AI_0V001	Transducer	6)T3	25	Y	25	40%	9.818325	y	100.00%	9.8183	PCc_HVPOSBATT	80.00%	1.963665
BATT'b'_PO_PC	Actuator	5)A5	0.5		0	40%	0	y	100.00%	0.0000	PCc_HVPOSBATT	80.00%	0
SPI ADC Inputs													
C'c'_AI_0V001	Measurement	6)M1	102	Y	102	40%	40.220334	Y	100.00%	40.2203	PCc_Batt_Bus_Compare	99.00%	0.40220334
SPI ADC Internal													
VMEAS_AI_TX	Transducer	6)T1	50	Y	50	40%	19.58715	Y	100.00%	19.5872	PCc_Batt_Bus_Compare	99.00%	0.1958715
SPI ADC Outputs													
VMEAS_AI_TX	Data	1)D1	3	Y	3	40%	1.089504	Y	100.00%	1.0895	PCc_Batt_Bus_Compare	99.00%	0.01089504
Module Management Inputs													
VMEAS_AI_TX	Data	1)D2	3	Y	3	40%	1.089504	Y	100.00%	1.0895	PCc_Batt_Bus_Compare	99.00%	0.01089504
M'm'_TRIP_FO_1Hz	Measurement	4)M4	3.5	Y	3.5	40%	0.62496	Y	100.00%	0.6250	Wdog	90.00%	0.062496
M'm'_TEST_DP	Data	5)D12	3	Y	3	40%	1.15236			0.0000			
Module Management Internals													
C'c'_AI_0V001	Parameter	1)P1	4.5	Y	4.5	40%	1.693395	Y	100.00%	1.6934	Wdog	90.00%	0.1693395
C'c'_OA_0V001	Parameter	1)P2	4.5	Y	4.5	40%	1.6986915	Y	100.00%	1.6987	Wdog	90.00%	0.16986915
M'm'_TRIP_DI_V	Actuator	2)A3	1	Y	1	40%	0.39312	Y	100.00%	0.3931			0.39312
M'm'_TRIP_DI_V	Output	5)O3	25	Y	25	40%	9.82575	Y	100.00%	9.8258			9.82575
Power Supply	General - PSU	1)PSU1	60	Y	60	40%	23.6412	Y	100.00%	23.6412	Wdog	90.00%	2.36412
Module Management Outputs													
M'm'_OA_TRIP_DP	Data	1)D3	3	Y	3	40%	1.15236	Y	100.00%	1.1524	PCc_Batt_Bus_Compare	99.00%	0.0115236
M'm'_TRIP_DO_V	Connection	5)C5	0.05	Y	0.05	40%	0.0198			0.0000			
BATT'b'_PO_PC	Output	4)O7	0.5	N	0	40%	0			0.0000			
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
HV Measurement Inputs													
S's'_HVPOS_AI_1V	Connection	1)C3	0.05		0	40%	0			0.0000			
S's'_HVBUS_AI_1V	Connection	1)C4	0.05		0	40%	0			0.0000			
HV Measurement Internal													
S's'_HVPOS_AI_1V	Measurement	1)M2	4.9		0	40%	0	Y		0.0000			0
S's'_HVPOS_AI_1V,HVPOS_BUS_/	Transducer	1)T2	14		0	40%	0			0.0000			
S's'_HVBUS_AI_1V	Measurement	1)M6	4.9		0	45%	0			0.0000			
S's'_HVPOS_AI_1V,	Parameter	1)P7	9		0	40%	0			0.0000			
Power Supply	General - PSU	1)PSU2	20		0	40%	0			0.0000			
HV Measurement Outputs													
S's'_HVPOS_AI_1V	Data	1)D7	3		0	40%	0			0.0000			
String Management Inputs													
M'm'_OA_TRIP_DP	Data	1)D5	6	Y	6	40%	2.30472	Y	100.00%	2.3047	PCc_Batt_Bus_Compare	99.00%	0.0230472
M'm'_TRIP_DO_V	Connection	5)C6	0.05	Y	0.05	40%	0.0198			0.0000			
M'm'_TRIP_DP	Data	4)D11	3		0	45%	0			0.0000			
String Management Internal													
S's'_TRIP_DP	Parameter	1)P8	9	Y	9	40%	3.38679	Y	100.00%	3.3868	Wdog	90.00%	0.338679
SAFETY_OK_DI_V	Measurement	5)M5	4	Y	4	40%	1.277136	Y	100.00%	1.2771			1.277136
M'm'_OK_DLY_DI_V	Transducer	5)T4	8	Y	8	40%	2.570904	Y	100.00%	2.5709			2.570904
Power Supply	General - PSU	1)PSU3	40	Y	40	40%	15.7608	Y	100.00%	15.7608	Wdog	90.00%	1.57608
String Management Outputs													
HVPOS1P_DHO_V	Output	7)O1	20	Y	20	40%	7.8804	Y	100.00%	7.8804	PCc_Batt_Bus_Compare	99.00%	0.078804
HVNEGN_DLO_V	Output	7)O2	20	Y	20	40%	7.8804	y	100.00%	7.8804			7.8804
M'm'_TEST_DP	Data	5)D12	3	Y	3	45%	1.296405			0.0000			
String Hardware Logic Inputs													
M'm'_OK_DLY_DI_V	Actuator	6)A6	12	Y	12	40%	4.71744	y	100.00%	4.7174			4.71744
String Hardware Logic outputs													
HVPOS1N_DLO_V	Output	7)O5	20	Y	20	40%	7.8804	y	100.00%	7.8804			7.8804
HVNEGP_DHO_V	Output	7)O6	20	Y	20	40%	7.8804	y	100.00%	7.8804			7.8804
Coils													
HVPOS1P_DHO_V	Actuator	7)A1	15	y	15	100%	12.72825	Y	100.00%	12.7283	PCc_Batt_Bus_Compare	99.00%	0.1272825
HVPOS1N_DHSO	Actuator	7)A4	15	y	15	100%	12.72825	y	100.00%	12.7283	PCc_Batt_Bus_Compare	99.00%	0.1272825
HVNEGN_DLO_V	Actuator	7)A2	15	y	15	100%	12.72825	y	100.00%	12.7283	PCc_Batt_Bus_Compare	99.00%	0.1272825
HVNEGP_DHO_V	Actuator	7)A7	15	y	15	100%	12.72825	y	100.00%	12.7283	PCc_Batt_Bus_Compare	99.00%	0.1272825
			597.15		**534.25**		**LFM =**	**89.9%**					**52.28**

The SPFM is now 97.3%, i.e. capable of being used to satisfy the safety goal at ASIL C and the LFM is 89.9% which again matches the ASIL C requirement and only 0.1% below that required for ASIL D.

This architecture satisfies a generic requirement for ASIL C for a BMS. Each vehicle application would have to be individually assessed but the Company investigating this system had performed a safety element out of context assessment and determined that ASIL C was required for the safety goal to maintain the cells within their operating area.

Having such a significant increase in SPFM on the final architecture poses the question 'Should this diagnostic capability have been added into the first architecture?' The reason for adding in this diagnostic capability late in the design is:

1) There are external methods in which the output of the BMS can be verified i.e. any external load on the HV bus can have a measurement system capable of verifying whether the contactors are open or closed. Although this is an independent system it was felt that it would complicate the overall vehicle design in that requirements would have to be placed on external systems and these tracked throughout a project. This makes the system less generic and harder to apply to different vehicle applications, especially when these are proof of concept designs.
2) To make the measurements, there are a number of measurement points that have to be added in hardware, all of which have to be isolated from the low voltage (12V) system.
3) The checks need to be sequenced which is not an insignificant amount of software development to ensure all of the failure modes can be diagnosed correctly.
4) Performing tests in sequence adds delays for closing and opening contactors to allow time for voltages to increase or decrease (in a normal start-up / shutdown sequence). Delays are considered a disadvantage in terms of starting and stopping the vehicle. However, the increase in safety achieved compared to a minor inconvenience would not prevent this sequence being implemented.

The PCc method would allow the designer to go back and run this analysis if necessary, i.e. take architecture 3 and add the contactor diagnostics as implement in architecture 7 and determine the projected SPFM and LFM architectural metrics. This was not performed as part of this work as the design was felt to satisfy all requirements for a generic (safety element out of context) design.

4.3.7 Results

The PCc analysis has taken the design through seven different candidate architectures with each one providing predicted SPFM and LFM values. To determine the accuracy of these predictions the final

SPFM and LFM values must be calculated. The process is the same as that discussed in 4.2.6, however, the number of components involved makes this a major task. The full analysis contains more than 2000 component failure modes to be analysed for architecture 7. Architectures 1 to 6 offer some reduction in these numbers but the task is of similar complexity. For brevity, only the Architecture 7 calculations are included in the appendices. The full SPFM calculations for Architecture 7 are shown in Appendix E8 – BMS SPFM Calculation – Architecture 7 and the LFM calculations in Appendix E9 – BMS LFM Calculation – Architecture 7.

The results are summarised below (Table 76). This shows the comparison between the SPFM and LFM predicted values achieved for each candidate architecture using the PCc method against the full SPFM and LFM values calculated as per the standard (BSI, 2011e).

Table 76: Battery Management System Calculation Comparison

		SPFM	LFM
Architecture 1	**PCC**	81.60%	71.95%
	Full	82.53%	71.43%
	Error	-0.93%	0.51%
Architecture 2	**PCC**	62.97%	75.86%
	Full	58.43%	76.36%
	Error	4.53%	-0.50%
Architecture 3	**PCC**	77.58%	76.25%
	Full	75.58%	77.64%
	Error	2.00%	-1.39%
Architecture 4	**PCC**	77.96%	79.64%
	Full	75.68%	81.68%
	Error	2.28%	-2.04%
Architecture 5	**PCC**	81.24%	84.45%
	Full	79.69%	83.49%
	Error	1.55%	0.96%
Architecture 6	**PCC**	82.18%	87.35%
	Full	80.48%	88.43%
	Error	1.70%	-1.07%
Architecture 7	**PCC**	97.31%	89.94%
	Full	97.09%	90.30%
	Error	0.22%	-0.36%

Before examining the detail of the results, it is very important to emphasise that when the PCc examples were being developed and calculated the effort required was very low compared to that of the full calculations. Ignoring the gathering / calculation of the failure rate data, simply analysing each component failure mode and determining the applicable diagnostic coverage for one of the

architectures took more than six man-months effort. This reduced for each subsequent architecture, but still required a significant amount of time.

The normal process would be to try and increase the SPFM and LFM architectural metrics with each iterative design. However, with the ease that a system can be quantified with the PCc method it was decided to analyse a software-based solution (Architecture 1) and a hardware based solution (Architecture 2) just to understand the differences. From architecture 3 onwards the normal process in improving the design was followed. The PCc quantification showed this to be the case as each iteration from architecture 3 onwards gave an improvement in both SPFM and LFM.

It is interesting that the SPFM dipped significantly moving from the software technique (Architecture 1) to the hardware technique (Architecture 2) but this is where several points need to be considered:

1) The SPFM achievable in hardware is typically lower as it is not possible to utilise as many different techniques with a simple hardware-based system
2) If the violation of the safety goal due to random hardware failures was analysed the probability of failure for the hardware system is likely to be significantly low as it uses a completely independent system. This may have driven the design in terms of failure rates but not (as indicated) be sufficiently robust in terms of architectural metrics.
3) The hardware system would be limited din how it could be configured compared to the software system where calibration tables could be downloaded into the microcontroller and modified as required.
4) Improvements are evident by utilising a combined approach. This is also likely to result in an overall improvement in the probability of random hardware failures as the hardware based system remains independent to the software based system.

These results were mirrored in the full design results for SPFM and LFM. The worst-case error in SPFM was 4.53% for architecture 2, the hardware based solution. This was due to optimistic assumptions in the PCc design that failure modes would be covered. In the final implementation it was not possible to justify these claims without resorting to additional software based diagnostics. As the aim of the architecture was to rely on hardware the additional software functionality was not included.

From architecture 3 onwards the worst case SPFM error is 2.28% and the worst case LFM error is -2.4%. In general, the PCc SPFM values are optimistic (see Figure 30) and the PCc LFM values pessimistic (see Figure 31). All the results are within acceptable limits and decisions can be made based on the PCc results to select the design to take forwards.

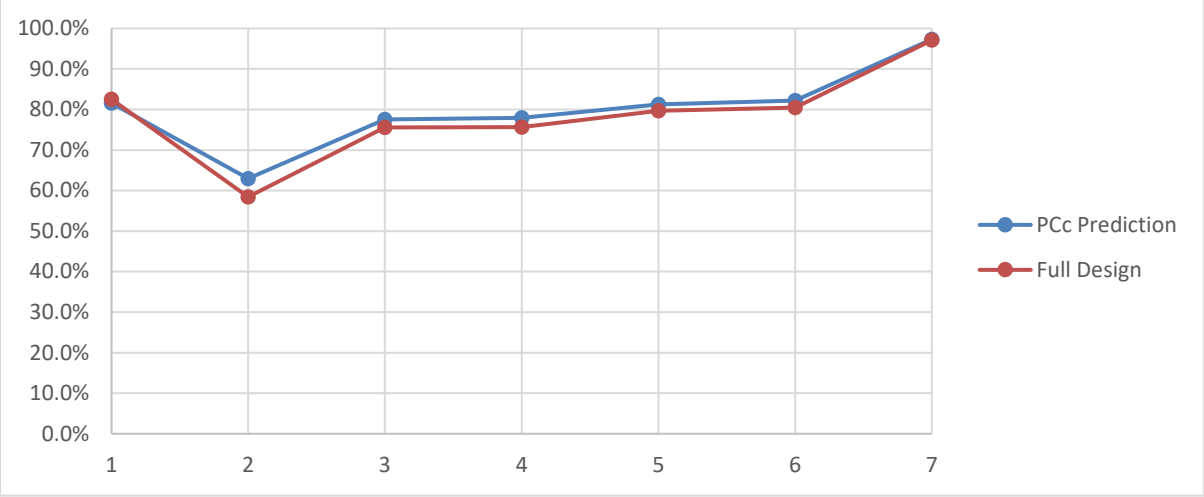


Figure 30: SPFM Comparison for the BMS

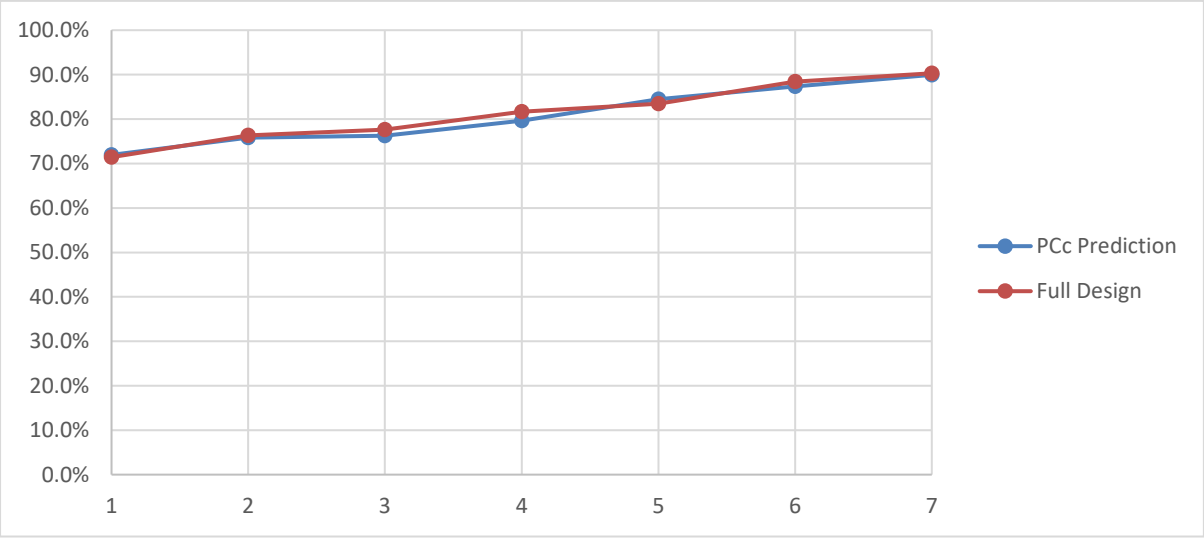


Figure 31: LFM Comparison for the BMS

The main point is that the average increases in architectural metrics for each iterative design architecture 3 onwards) provided by the PCc method agrees with the average increases in the full SPFM and LFM values. In no cases does an increase in the PCc values result in a decrease when the full design calculations are completed.

The closeness of result is considered to be the based on the same discussion for the isolation measurement system (4.2.6).

4.4 Fuel Cell Control System

A Fuel Cell Control system was chosen as it is a relatively complex control system where a large number of control elements interact and all are required in order to deliver a controlled power output from the system.

In order to apply the method in a different way, the approach with the fuel cell is to examine the system as described in 4.4.2 and look at the possible PCcs that can be applied based on an assumption of sensors, actuators, microcontroller and published data on fuel cell control system control as discussed by Kunusch et al (Kunusch C, 2012). The data is quite restricted but not dissimilar to that available when considering new technology or proof of concept. Generally, at initial discussion, engineers would have an idea that the ASIL level required would be high (ASIL 'C' or ASIL 'D') based on hydrogen leakage and explosion even without performing a detailed HARA, this in turn leads to a preliminary design to be considered. What is not normally possible is an analysis to determine what ASIL can be achieved with the final system based on this limited amount of information.

In the majority of applications, whether this is for stationary power or for automotive applications, the Fuel Cell system would normally provide energy via a DCDC converter into a small battery in order to provide a buffered output to the load. An example is discussed by (Yu X., 2007) showing various examples aimed at electric power applications. Similar architectures are applicable to automotive applications.

The fuel cell control system needs to control or monitor a number of parameters:

1) Hydrogen supply
2) Air supply
3) Cell temperatures
4) Voltage output
5) Output current limit
6) Cell voltage monitoring
7) Exhaust dilution of hydrogen

Failures of the any above may lead to violation of several different safety goals but when considered for delivering energy into the load all play a role. Depending on the application i.e. range extension or motive power in automotive applications the ASIL target for controlled output will vary.

Many of the safety issues relating to fuel cell powered vehicles have been researched (The International Consortium for Fire, Safety, Health and the Environment, 2011). This shows the wide range of issues from storage of hydrogen, the voltage output, refuelling the vehicle and the requirements for early leak detection.

The PCc estimation for the fuel cell control system was performed based on a few different assumptions:

1) No additional safety features will be included in the PCc analysis other than those that can be achieved with existing sensors / measurements.
2) Estimations would need to be made for failure rates where necessary as many components did not have failure rate data available from manufacturers.
3) Diagnostic coverage would be realistic based on available diagnostics available with the microcontroller and existing feedback means

The above makes the quantification realistic as a first pass estimate of achievable SPFM and LFM on a theoretical design that can be used for proof of concept.

4.4.1 Safety Goal Definition

4.4.1.1 Aim – Maintain the power output within the Fuel Cell System Operating Range.

When performing a hazard identification study on a Fuel Cell system there are likely to be a number of hazards relating to the control of hydrogen, the mixing of hydrogen and air in the exhaust dilution system, temperature control of the cells, operating voltage of the cells etc. Some of these are likely to have relatively high ASIL targets due to the high severity and exposure classifications and limited controllability. One safety goal that impacts on these control sub-systems is that of maintaining the required power output. For general motive power applications, for example, a range extender, this has a lower ASIL as the severity of a failure in this system is likely to result in reduced range rather than total loss of drive (subject to a full failure mode analysis). If consideration was being given to a drone then a higher ASIL is likely to result as due to weight restrictions it may only have sufficient battery power to land safely without the additional range coverage provided by the fuel cell.

This raises an interesting question regarding what architectural metrics can be achieved with an initial concept design. This is at the initial idea stage when deciding whether it is viable setting up a Research and Development project. PCc quantification metrics can be applied in this situation in order to assess likely architectural changes in a design in order to achieve a required ASIL. Without PCc quantification, this measure would be very difficult to predict and may take many months of obtaining accurate information and detailed architecture design and analysis at the hardware

component level. With PCc quantification this process can be achieved in approximately 120 hours and based on previous results the predication will be sufficiently accurate to base a decision on whether to initiate the project and take the design through a full BS ISO 26262 development process or else consider different architectures.

4.4.1.2 Safety Goal.

Persons shall not be exposed to any unreasonable risk due to the fuel cell not being able to supply power at the demanded voltage / current targets.

This assumes that the power demand by the load fall within the operating range of the Fuel Cell system.

4.4.2 System Description

The Fuel cell system diagram is shown in Figure 32. Each of the sub-systems involved in supplying power according to the safety goal are described in more detail below.

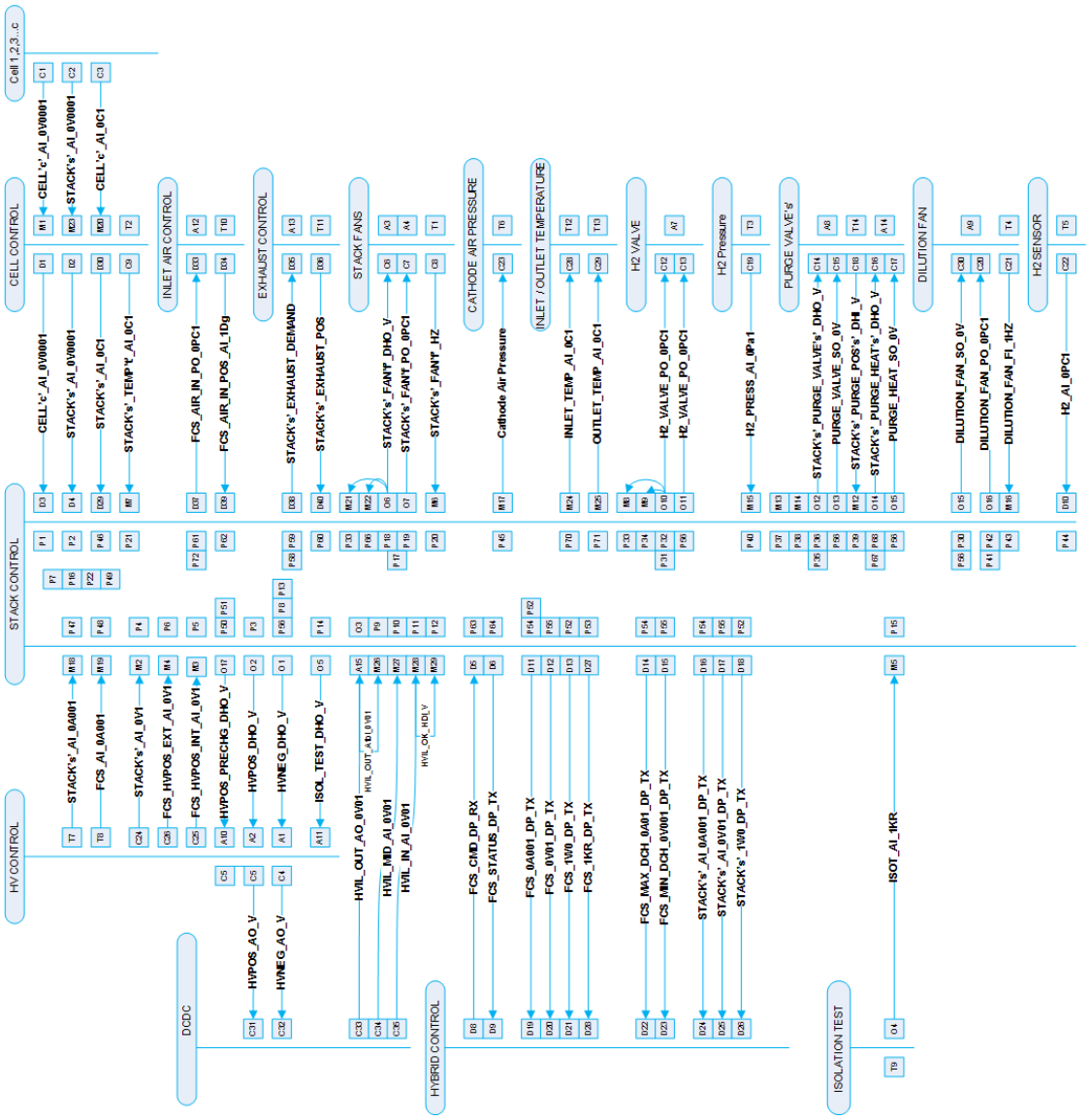


Figure 32: Fuel Cell System Diagram

4.4.2.1 Cell 1,2,3…c

These are the individual voltage measurements, like those used for Battery Management Systems. An initial review shows that analogue front end (AFE) devices from MAXIM such as the MAX14920/14921 (Maxim Integrated, 2014) or Linear Technology such as the LTC6804-1/LTC6804-2 (Linear Technology, 2016) multi-cell battery monitors. Both have similar characteristics, however discussions with Linear Technology indicate availability of functional safety relevant data that would be useful in a fully compliant development process. Both companies also have devices specific for fuel cell monitoring but this data is only available through a non-disclosure agreement (NDA) and so not included in this Thesis.

Cell voltage monitoring is critical as it can be used to detect a number of failures. This can initially exhibit as losses in efficiency but ultimately lead to catastrophic cell failure (Rama, 2008).

Temperature measurement is initially estimated to use simple Negative Temperature Coefficient (NTC) thermistors.

4.4.2.2 Cell Control

This handles conversion of data from the AFE (4.4.2.1) to a form suitable for processing by the Stack Control (4.4.2.7) sub-system. For high integrity systems, a companion chip from Linear Technology, the LTC6820 (Linear Technology, 2013) isoSPI device is suitable.

4.4.2.3 Inlet Control, Exhaust Control and Stack Fans

These sub-systems make up the air control path. The fans pull the air through the system with the path being an inlet filter, inlet control such as a louvre or iris, though the fuel cell, through the fan and finally out through the exhaust control which again may be a louvre or iris. Air control is required to provide sufficient oxygen to the fuel cell stack and also control the temperature of the stack.

4.4.2.4 Hydrogen (H_2) Valve, Hydrogen Pressure and Purge valve

The hydrogen valve and purge valve control the flow of hydrogen into the fuel cell stack and allow purging of the hydrogen into the exhaust dilution system. As the hydrogen has a high moisture content the purge valve also allows any collected water to be expelled as part of the hydrogen purge. The hydrogen pressure sensor allows pressure within the stack to be monitored.

4.4.2.5 Dilution Fan

As hydrogen is vented as part of the hydrogen pressure control. In order to maintain hydrogen safety, it is important that the hydrogen can't accumulate in quantities that would exceed the regulation for fuel cells (BSI, 2012). This is achieved with a dilution fan that forces air through the exhaust ducting and allows the hydrogen to disburse to ambient at very low concentration levels.

4.4.2.6 Hydrogen (H_2) Sensor

Monitoring of hydrogen concentrations in the exhaust is possible (AMS AG, 2015), although generally expensive for high reliability sensors that are not prone to poisoning by contaminants in the air and suitable for use in automotive applications. The lower flammability limit of hydrogen (BOC, 2015) is 4% by volume and so continuous monitoring may offer a solution to failures in dilution or the purge valve etc.

4.4.2.7 Stack Control

The Stack Control is effectively the main Fuel cell system controller and is responsible for the overall management. All inputs and outputs are routed to this either directly or via communications networks such as LIN bus or CAN bus.

There are assorted options for the microcontroller. The choice is constrained by the usual input / output pin functionality, performance and cost. In terms of functional safety, other factors need to be considered depending on the ASIL target. As this exercise is to determine what can be achieved with a conceptual design and it is known that some of the ASIL targets will be C or D a reasonable assumption is that dual-core architecture configuration (Leteinturier, 2008), for example, a lock-step microcontroller will be required. Lock-steps have a high immunity to random hardware failures due to their two cores that operate out of phase by a fixed number of clock cycles and are physically at 90^{O} to each other. This gives a high level of immunity to transient and common cause failures as it would be very unlikely for both cores to be affected in a way that was not detected by the comparator that verifies the outputs from the two cores have the same results (once back in phase). Lock-step microcontrollers have many additional diagnostic functions such as Cyclic Redundancy Check (CRC) hardware, peripheral diagnostics, memory protection and often a companion chip with an intelligent question / answer window watchdog.

Several manufacturers have comparable solutions such as Renesas (Renesas Electronics Europe, 2016), Infineon (Infineon Technologies AG, 2014) and Texas Instruments (Texas Instruments, 2014). For the purposes of this design the Texas Instruments Hercules TMS570 (see 4.2.5.4.3) was selected.

4.4.2.8 DCDC Converter

In a vehicle application the DCDC converter couples the two power sources (Karaki S, 2015) which in this case are the fuel cell and the battery. The DCDC converter primarily feeds a battery or during peak vehicle power requirements the energy may be delivered directly to the propulsion system. This imposes a number of requirements on the battery such as continuous power, peak power, charge rates for regenerative braking (Markel T, 2003). This in turn imposes requirements on the fuel cell to deliver power.

Another operation not discussed by the authors above, where the battery is required to maintain power to the vehicle is during fuel cell recovery methods. This is achieved by eliminating air supply to the fuel cells and applying a load to the fuel cell outputs (Choo, 2015).

4.4.3 Fault Consideration

As the approach was being applied to concept with limited definition, it was decided not to perform an FMEA but rely on PCcs developed from two approaches:

- Failure modes that would be detected by diagnostic techniques described in ISO 26262 Part 5 (BSI, 2011e).

- Standard PCc techniques that had been developed in previous designs i.e. the Isolation Tester (4.2) and Cell Management system (4.3). This is based on the fact that PCcs would be developed to be generic so that they can be re-used on future projects, for example monitoring range on a sensor or monitoring current and voltage on an output that is driving an actuator.

4.4.4 System Analysis

To aid discussion in the Thesis, the system design was broken down into a number of sub-systems:

1) Voltage and current based measurement and control.
2) Air flow and temperature control.
3) Hydrogen delivery control, dilution and fuel cell purging.
4) Control parameters and data.
5) High Voltage Interlock (HVIL) and Isolation testing.

Each sub-system is discussed below.

4.4.4.1 Voltage and Current Based Measurement and Control Classified Signals

The system diagram for signals and elements relating to this sub-system are shown in Figure 33.

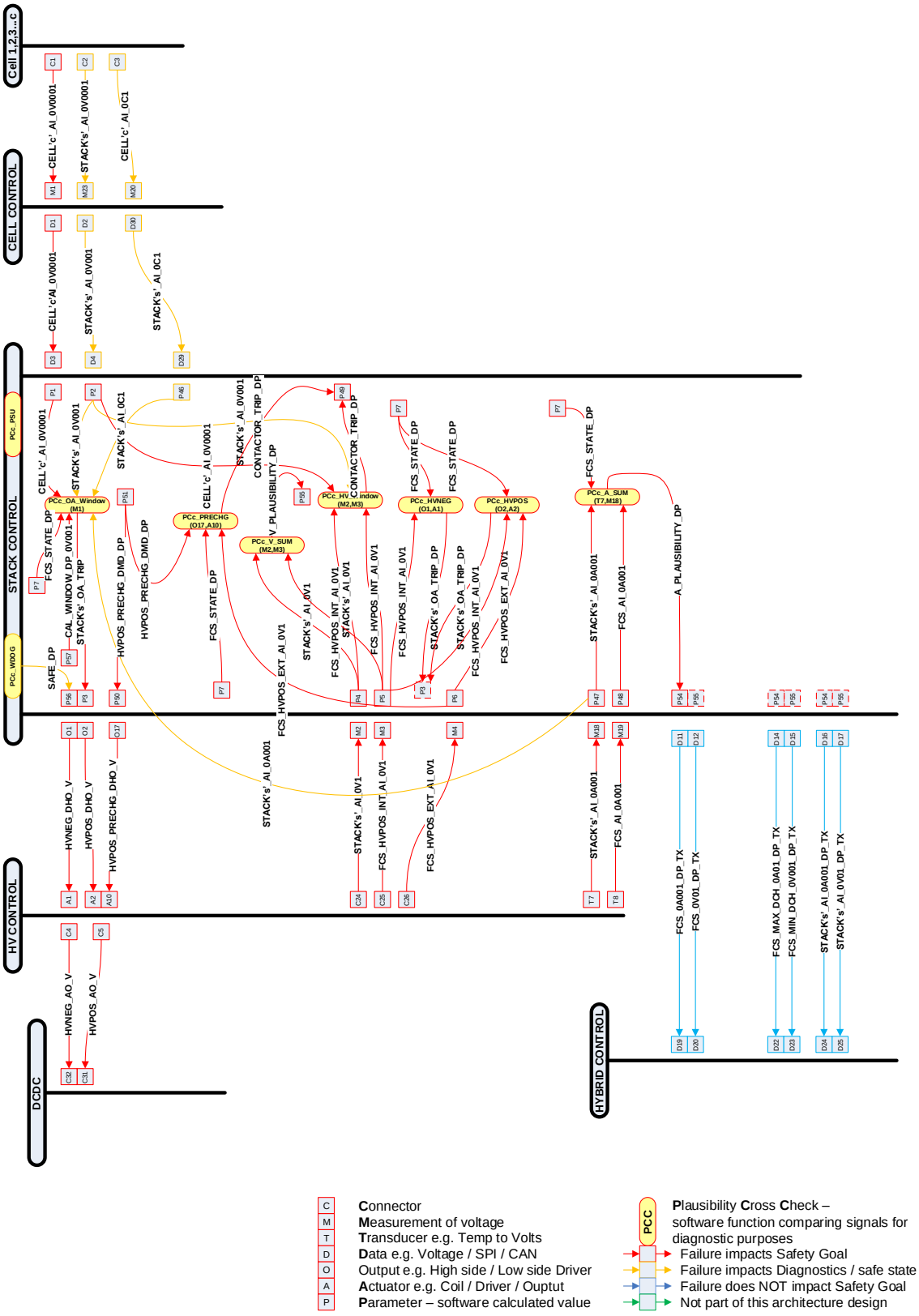


Figure 33: Voltage and Current Sub-system

To perform the analysis many signals are defined which are connected between the critical elements. For clarity, only signals for this sub-system (Figure 33) are defined in this section.

4.4.4.1.1 Cell1,2,3….'c'.

4.4.4.1.1.1 C1 – CELL'c'_AI_0V0001

The connection to each of the cells to facilitate individual voltage measurement. Note a common 0V connection is assumed through the frame for cell and stack measurement and so not included as a separate connection in this architecture.

4.4.4.1.1.2 C2 – STACK's'_AI_0V0001

The connection to the top of the stack 's' to facilitate individual stack voltage measurement.

4.4.4.1.1.3 C3 – CELL'c'_AI_0C1

The connection to each of the cells to facilitate temperature measurement. Thermal analysis may indicate that cells can be monitored as groups in a more cost-effective design but this is not assumed in this architecture.

4.4.4.1.2 Cell Control.

4.4.4.1.2.1 M1 and D1– CELL'c'_AI_0V0001

The measurement (M1) by the AFE of each of the individual cell voltages. This is made available to the Stack Control system as data (D1) over an SPI connection.

4.4.4.1.2.2 M23 and D2– STACK's'_AI_0V0001

The measurement (M23) by the cell control system of the overall stack voltage which is then transmitted over SPI (D2).

4.4.4.1.2.3 M20 and D30 – CELL'c'_AI_0C1

The temperatures of the cells are measured (M20) and the cell control system converts this to a calibrated temperature representing the overall stack temperature. The calibration is based on previous thermal analysis and the assembly pattern on the individual cells within the stack. Data is transmitted over SPI (D30).

4.4.4.1.3 Stack Control Inputs.

4.4.4.1.3.1 D3 and P1– CELL'c'_AI_0V0001

The data (D3) received and converted to an internal array of parameters (P1) representing individual cell ('1' to 'c') voltages.

4.4.4.1.3.2 D4 and P2– STACK's'_AI_0V0001

The data (D4) received and converted to an internal array of parameters (P2) representing individual stack ('1' to 's') voltages.

4.4.4.1.3.3 D29 and P46 – CELL'c'_AI_0C1

The data (D29) received and converted to an internal array of parameters (P46) representing individual stack ('1' to 's') temperatures.

4.4.4.1.3.4 M2 and P4 – STACK's'_AI_0V1

The measurement (M2) by the Stack Control system of the overall stack voltage which is then converted to an internal array of parameters (P4) representing each individual stack ('1' to 's') voltage.

4.4.4.1.3.5 M3 and P5 – FCS_HVPOS_INT_AI_0V1

The measurement (M3) for the stack total voltage internal to the Fuel cell system (prior to the HV contactors) which is then converted to an internal parameter (P5) representing the output voltage.

4.4.4.1.3.6 M4 and P6 – FCS_HVPOS_EXT_AI_0V1

The measurement (M4) for the stack total voltage external to the Fuel Cell system (on the output of the HV contactors) which is then converted to an internal parameter (P6) representing the output voltage. This is also capable of measuring the load voltage prior to closing or after opening the contactors.

4.4.4.1.3.7 M18 and P47 – STACK's'_AI_0A001

The measurement (M18) of each individual stack ('1' to 's') current converted to an internal parameter (P47).

4.4.4.1.3.8 M19 and P48 – FCS_AI_0A001

The measurement (M19) of the total FCS current converted to an internal parameter (P48).

4.4.4.1.4 Stack Control Internal.

4.4.4.1.4.1 P49 – CONTACTOR_TRIP_DP

An internal parameter (P49) that indicates that a contactor has tripped. The trip status is defined further as each of the applicable PCcs are discussed.

4.4.4.1.4.2 P7 – FCS_STATE_DP

An internal parameter (P7) representing the main state machine enumerated type for the Fuel Cell system. This is used for all monitoring and control functions for starting up, running and shutting down the Fuel Cell system.

4.4.4.1.4.3 P51 – HVPOS_PRECHG_DMD_DP

An internal parameter (P51) indicating the demand for a pre-charge. When set, the Fuel Cell Control System (FCCS) will pre-charge the HV bus supplying the load with a limited current. This is designed to limit the inrush current and protect any capacitor banks in the DCDC converter.

4.4.4.1.4.4 P55 – V_PLAUSIBILITY_DP

An internal parameter (P55) which is set when the voltage plausibility PCc fails.

4.4.4.1.4.5 P57 – CAL_WINDOW_DP_0V001

An internal calibration structure (P57) which is used to determine minimum and maximum voltage ranges for the stacks (‘1’ to ‘s’).

4.4.4.1.4.6 P3 – STACK's'_OA_TRIP_DP

An internal parameter (P3) which is used indicate when a stack (‘1’ to ‘s’) voltage is outside of its operating area.

4.4.4.1.4.7 P54 – A_PLAUSIBILITY_DP

An internal parameter (P54) which is set when the current (Amperes) plausibility PCc fails.

4.4.4.1.5 Stack Control Outputs.

4.4.4.1.5.1 O1 and P56 – HVNEG_DHO_V

An internal parameter (P56) indicating that the stack controller watchdog monitor has tripped. This independently opens the HVNEG_DHO_V contactor (O1).

4.4.4.1.5.2 O2 and P3 – HVPOS_DHO_V

An internal parameter (P3) that will open the contactor (HVPOS_DHO_V (O2)) if the stack ’s’ voltage is outside of its operating area. Under normal circumstances the contactor will open and close under the command of the main state machine (FCS_STATE_DP).

4.4.4.1.5.3 O17 and P50 – HVPOS_PRECHG_DHO_V

This output delivers limited current to the HVPOS output (HVPOS_AO_V) as demanded by the FCS_STATE_DP.

4.4.4.1.6 HV Control.

4.4.4.1.6.1 A1 - HVNEG_DHO_V and C4 – HVNEG_AO_V

The actuator (A1) is the main negative contactor used to switch the negative side of the High Voltage output to the load (DCDC).

4.4.4.1.6.2 A2 - HVPOS_DHO_V and C5 – HVPOS_AO_V

The actuator (A2) is the main positive contactor used to switch the positive side of the High Voltage output to the load (DCDC).

4.4.4.1.6.3 A10 – HVPOS_PRECHG_DHO_V

The output that self-limits current to HVPOS output (HVPOS_AO_V) as demanded by the FCS_STATE_DP. The self-limit can be achieved by a Positive Temperature Coefficient (PTC) resistor.

4.4.4.1.6.4 C24 – STACK's'_AI_0V1

The connection (C24) for the overall stack voltage

4.4.4.1.6.5 C25 - FCS_HVPOS_INT_AI_0V1

The connection (C25) for the stack total voltage internal to the FCCS.

4.4.4.1.6.6 C26 – FCS_HVPOS_EXT_AI_0V1

The connection (C26) for the stack total voltage external to the FCCS.

4.4.4.1.6.7 T7 – STACK's'_AI_0A001

The current sensor (T7) for each individual stack ('1' to 's') current.

4.4.4.1.6.8 T8 – FCS_AI_0A001

The current sensor (T8) for the total FCS current.

4.4.4.1.7 DCDC.

4.4.4.1.7.1 C32 – HVNEG_AO_V

The connection (C32) to the DCDC converter. This is effectively outside of the boundary of the FCCS but critical to successful operation in an automotive application.

4.4.4.1.7.2 C31 – HVPOS_AO_V

The connection (C31) to the DCDC converter. This is effectively outside of the boundary of the FCCS but critical to successful operation in an automotive application.

4.4.4.1.8 Hybrid Control

This is shown for completeness in the FCCS diagram but not required as part of the safety case for the FCCS as the Hybrid Control lies outside of the FCS boundary.

4.4.4.2 Air Flow and Temperature Control Classified Signals

The air flow and temperature related elements and signals are shown in Figure 34.

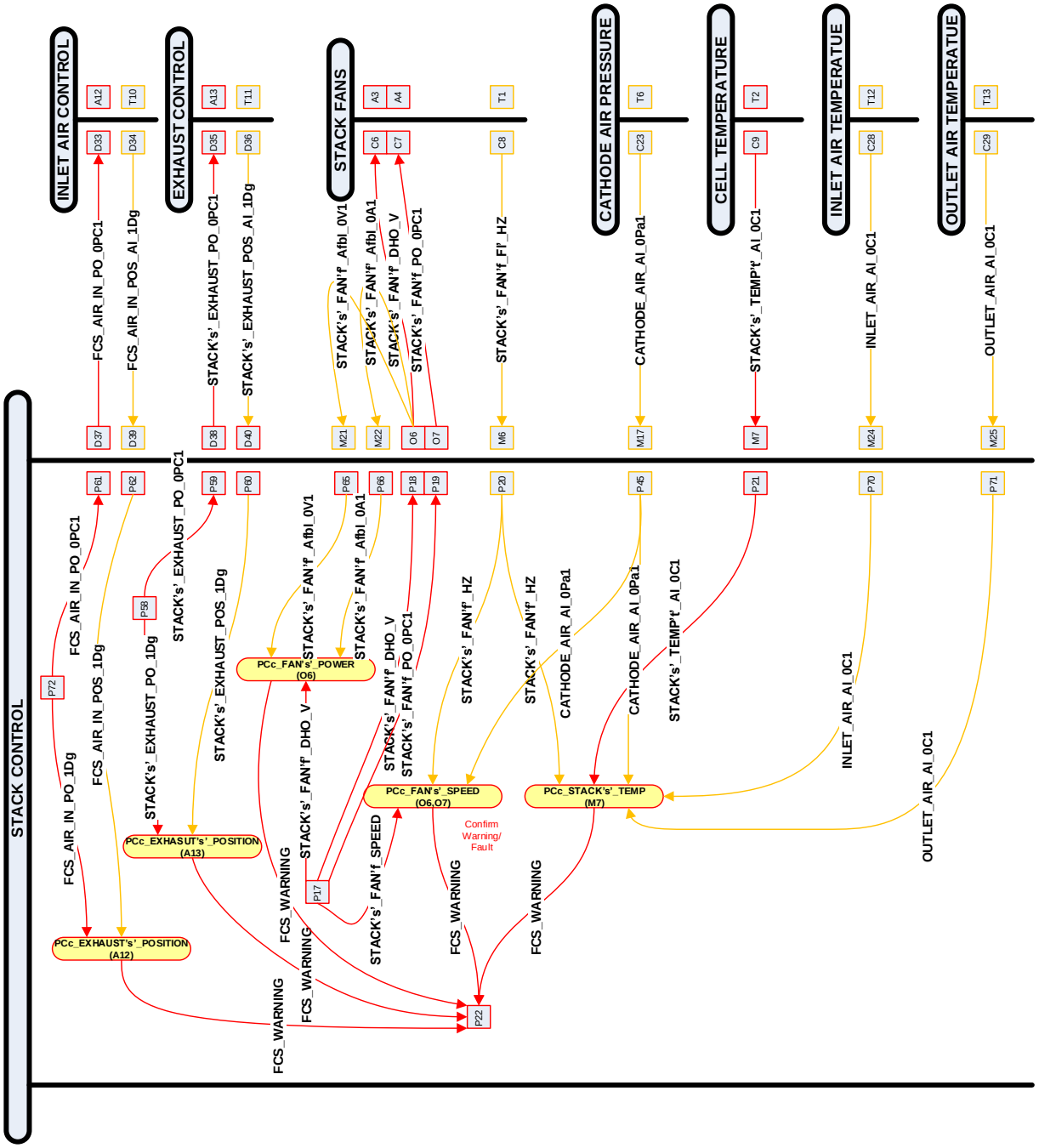


Figure 34: Air Flow and Temperature Control Sub-system

4.4.4.2.1 Inlet air Control.

4.4.4.2.1.1 A12 and D33 – FCS_AIR_IN_PO_0PC1

The PWM output that controls the angular position of the air input to the fuel cell stack. The 0.1% duty cycle resolution provides 1000 available steps for control.

4.4.4.2.1.2 T10 and D34 – FCS_AIR_IN_PO_0PC1

The FCS_AIR_IN_POS_AI_1Dg signal provides feedback on the control. The actual control loop runs on temperature control and so the feedback is used as a plausibility check rather than having to match the accuracy of the PWM output.

4.4.4.2.2 Exhaust Control.

4.4.4.2.2.1 A13 and D35 – STACK's'_EXHAUST_PO_0PC1

The PWM output that controls the angular position of the air exhaust the for each fuel cell stack. The 0.1% duty cycle resolution provides 1000 available steps for control.

4.4.4.2.2.2 T11 and D36 – STACK's'_EXHAUST_POS_AI_1Dg

The STACK's'_EXHAUST_POS_AI_1Dg signal provides feedback on the control for each individual fuel cell stack. The actual control loop runs on temperature control and so the feedback is used as a plausibility check rather than having to match the accuracy of the PWM output.

4.4.4.2.3 Stack Fans.

4.4.4.2.3.1 A3 and C6 – STACK's'_FAN'f'_DHO_V

The high side digital output that controls power to the fan for an individual fuel cell stack.

4.4.4.2.3.2 A4 and C7 – STACK's'_FAN'f'_PO_0PC1

Often, to maintain an evenly distributed air flow across the stack a number of fans (1 to 'f') are used to control air flow. The PWM output that controls the individual fan speed to fan 'f' the for each individual fuel cell stack 's'. The 0.1% duty cycle resolution provides 1000 available steps for control.

4.4.4.2.3.3 T1 and C8 – STACK's'_FAN'f'_FI_1HZ

The STACK's'_FAN'f'_FI_1HZ signal provides feedback on the fan speed of each individual fan. This allows diagnostics in terms of fan running / not running and actual speed.

4.4.4.2.4 Cathode Air Pressure.

4.4.4.2.4.1 T6 and C23 – CATHODE_AIR_AI_0Pa1

The cathode air pressure is effectively the air pressure at the input to the Fuel Cell system and can be used to determine pressure drop across the filters.

4.4.4.2.5 Cell Temperature.

4.4.4.2.5.1 T2 and C9 – STACK's'_TEMP't'_AI_0C1

The stack (1 to 's') is an overall stack temperature measurement. This depends on the position the transducer is mounted in the stack; typically, calibration allows it to be used to interpolate individual cell temperatures.

4.4.4.2.6 Inlet Air Temperature.

4.4.4.2.6.1 T12 and C28 – INLET_AIR_AI_0C1

The system inlet air temperature is an average temperature for the air being drawn into the Fuel Cell system. As this is ambient air from the surroundings, the temperature is assumed to be representative of the air temperature flowing into each stack (1 to 's').

4.4.4.2.7 Outlet Air Temperature.

4.4.4.2.7.1 T13 and C29 – OUTLET_AIR_AI_0C1

This is purely a monitor for diagnostic purposes and not used for control so an average for all of the stacks (1 to 's') is used.

4.4.4.2.8 Stack Control Inputs.

4.4.4.2.8.1 D39 and P62 – FCS_AIR_IN_POS_AI_1Dg

CAN data converted to an internal parameter for the FCS_AIR_IN_POS_AI_1Dg signal.

4.4.4.2.8.2 D40 and P60 – STACK's'_EXHAUST_POS_1Dg

CAN data converted to an internal parameter for the STACK's'_EXHAUST_POS_1Dg signal.

4.4.4.2.8.3 M21 and P65 – STACK's'_FAN'f'_AfbI_0V1

Measurement of the STACK's'_FAN'f'_AfbI_0V1 voltage feedback signal and conversion to an internal parameter for fan actuator diagnostic purposes.

4.4.4.2.8.4 M22 and P66 – STACK's'_FAN'f'_AfbI_0A1

Measurement of the STACK's'_FAN'f'_AfbI_0A1 current feedback signal and conversion to an internal parameter for fan actuator diagnostic purposes.

4.4.4.2.8.5 M6 and P20 – STACK's'_FAN'f'_FI_1HZ

Measurement of the STACK's'_FAN'f'_FI_1HZ speed signal and conversion to an internal parameter for fan speed / air flow diagnostic purposes.

4.4.4.2.8.6 M17 and P45 – CATHODE_AIR_AI_0Pa1

Measurement of the CATHODE_AIR_AI_0Pa1 signal and conversion to an internal parameter for cathode air pressure diagnostic purposes.

4.4.4.2.8.7 M7 and P21 – STACK's'_TEMP't'_AI_0C1

Measurement of the STACK's'_TEMP't'_AI_0C1 signal and conversion to an internal parameter for monitoring stack temperature as part of the temperature control loop.

4.4.4.2.8.8 M24 and P70 – INLET_AIR_AI_0C1

Measurement of the INLET_AIR_AI_0C1 signal and conversion to an internal parameter for monitoring inlet air temperature for diagnostic purposes.

4.4.4.2.8.9 M25and P71 – OUTLET_AIR_AI_0C1

Measurement of the OUTLET_AIR_AI_0C1 signal and conversion to an internal parameter for monitoring outlet air temperature for diagnostic purposes.

4.4.4.2.9 Stack Control Internals.

4.4.4.2.9.1 P58 - FCS_AIR_IN_PO_1Dg

An internal parameter in degrees that is converted to a PWM value to control the inlet air damper.

4.4.4.2.9.2 P72 - STACK's'_EXHAUST_PO_1Dg

An internal parameter in degrees that is converted to a PWM value to control the outlet (exhaust) air damper.

4.4.4.2.9.3 P17 - STACK's'_FAN'f'_SPEED

An internal parameter for controlling the fan speed digital outputs for power and the PWM outputs for speed control. This would be linked to the main FCCS state machines and temperature control loops.

4.4.4.2.9.4 P22 - FCS_WARNING

In order to simplify the diagrams, the FCS warning is a genic signal used to indicate a warning in the system. This would use all of the diagnostic routes to maintain a full warning / error list and these would either shut down or reduce power output – both of which deviate the safety goals and so a single warning flag is considered sufficient for the PCc analysis.

4.4.4.2.10 Stack Control Outputs.

4.4.4.2.10.1 P61 and D37 – FCS_AIR_IN_PO_0PC1

Internal parameter for the FCS_AIR_IN_PO_0PC1 signal output on CAN.

4.4.4.2.10.2 P59 and D38 – STACK's'_EXHAUST_PO_0PC1

Internal parameter for the STACK's'_EXHAUST_PO_0PC1 signal output on CAN.

4.4.4.2.10.3 P18 and O6 – STACK's'_FAN'f'_DHO_V

Internal parameter for the STACK's'_FAN'f'_DHO_V signal which drives the power output to the fan (1 to 'f') on each stack. This provides an independent shutdown path to the PWM outputs.

4.4.4.2.10.4 P19 and O7– STACK's'_FAN'f_PO_0PC1

Internal parameter for the STACK's'_FAN'f_PO_0PC1 signal which drives the PWM output to the fan (1 to 'f') on each stack for speed / air flow control.

4.4.4.3 Hydrogen Delivery Control, Dilution and Fuel Cell Purging Classified Signals

The hydrogen delivery related elements and signals are shown in Figure 35.

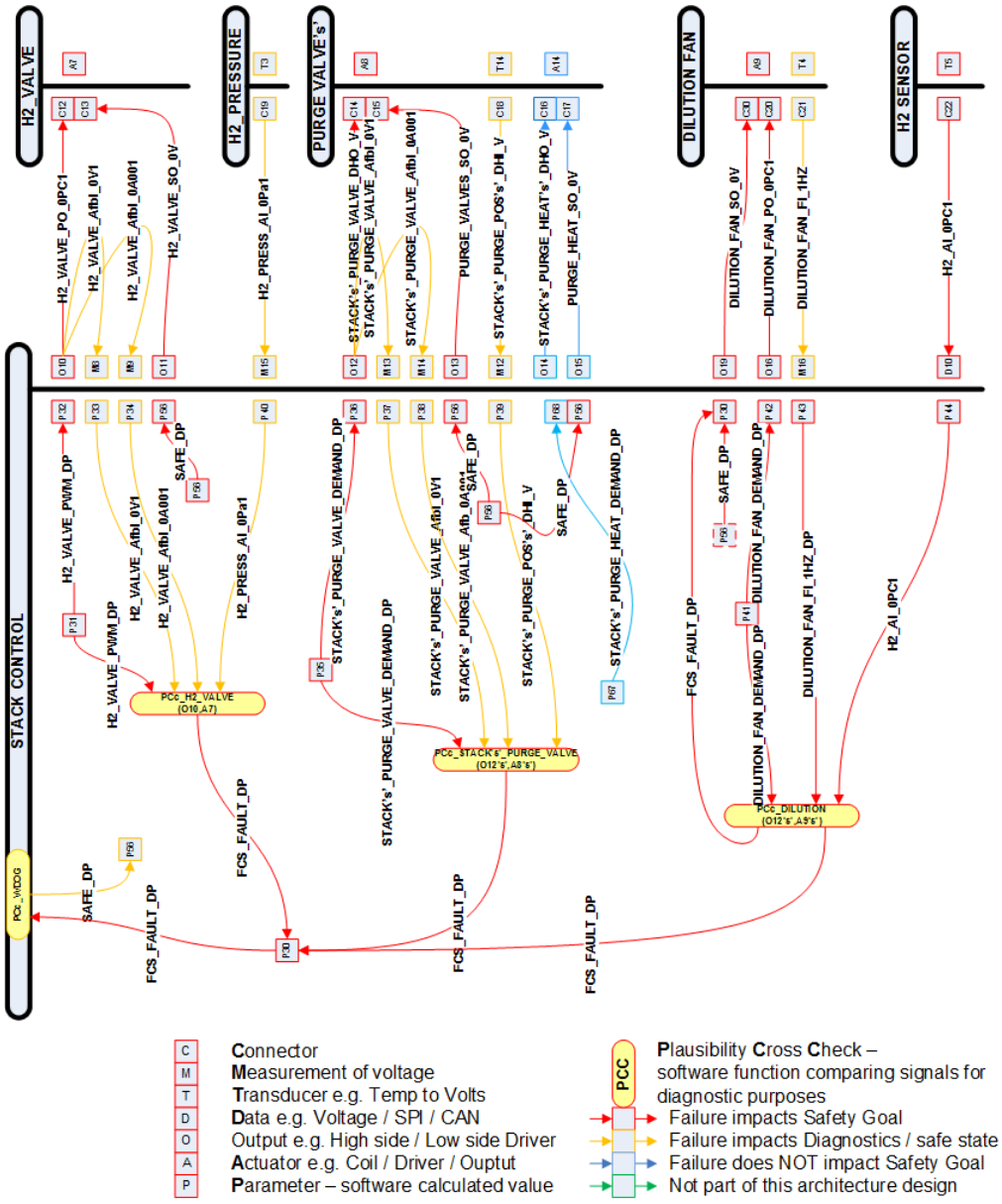


Figure 35: Hydrogen Control Sub-system

4.4.4.3.1 Hydrogen Valve (H2_VALVE)

4.4.4.3.1.1 C12 and A7 - H2_VALVE_PO_0PC1

The connection (C12) for the hydrogen valve (A7).

4.4.4.3.1.2 C13 and A7 - H2_VALVE_SO_0V

The 0V return (C13) for the hydrogen valve (A7).

4.4.4.3.2 Hydrogen Pressure (H2_PRESSURE)

4.4.4.3.2.1 C19 and T3 - H2_PRESS_AI_0Pa1

The H2_PRESS_AI_0Pa1 measure at the input to the Fuel Cell system. This allows diagnostics to be performed on the hydrogen valve.

4.4.4.3.3 Purge Valve (PURGEVALVE's')

4.4.4.3.3.1 C14 and A8 - STACK's'_PURGE_VALVE_DHO_V

The connection (C14) and purge value (A8) for the STACK's'_PURGE_VALVE_DHO_V signal allowing hydrogen to be purged from the system.

4.4.4.3.3.2 C15 and A8 - PURGE_VALVES_SO_0V

The PURGE_VALVES_SO_0V is the 0V return signal for the purge valve.

4.4.4.3.3.3 C18 and T14 - STACK's'_PURGE_POS's'_DHI_V

The STACK's'_PURGE_POS's'_DHI_V signal indicates the position (open or closed) of the purge valve which is used to diagnose possible problems with the purge valve control including mechanical failures that prevent the purge valve from closing.

4.4.4.3.3.4 C16 and A14 - STACK's'_PURGE_HEAT's'_DHO_V

The STACK's'_PURGE_HEAT's'_DHO_V controls the heater in the purge valve to ensure that it can be opened / closed correctly in in very low ambient (freezing) conditions.

4.4.4.3.3.5 C17 and A14 - STACK's'_PURGE_HEAT's'_SO_0V

The STACK's'_PURGE_HEAT's'_SO_0V return signal for the purge valve heater.

4.4.4.3.4 Dilution Fan (DILUTION_FAN))

4.4.4.3.4.1 C30 and A9 - DILUTION_FAN_SO_0V

The 0V return for the dilution fan.

4.4.4.3.4.2 C20 and A9 - DILUTION_FAN_PO_0PC1

The speed control for the dilution fan.

4.4.4.3.4.3 C21 and T4 - DILUTION_FAN_FI_1HZ

Monitoring of the dilution fan speed for diagnostic purposes.

4.4.4.3.5 H2 Concentration (H2_SENSOR)

4.4.4.3.5.1 C22 and T5 - H2_AI_0PC1

The transducer (hydrogen sensor) that measures hydrogen concentration in the exhaust. Typically measures low concentrations of hydrogen as a percentage of the lower explosive limit (LEL).

4.4.4.3.6 Stack Control Inputs (STACK_ CONTROL)

4.4.4.3.6.1 P33 and M8 - H2_VALVE_AfbI_0V1

Voltage monitoring (H2_VALVE_AfbI_0V1) of the supply to the hydrogen valve.

4.4.4.3.6.2 P34 and M9 - H2_VALVE_AfbI_0A001

Current monitoring (H2_VALVE_AfbI_0A001) of the hydrogen valve.

4.4.4.3.6.3 P40 and M15 - H2_PRESS_AI_0Pa1

The H2_PRESS_AI_0Pa1 as measured at the input to the Fuel Cell system converted to a scaled parameter for internal diagnostics.

4.4.4.3.6.4 P37 and M13 - STACK's'_PURGE_VALVE_AfbI_0V1

Voltage monitoring (STACK's'_PURGE_VALVE_AfbI_0V1) for each stack purge valve.

4.4.4.3.6.5 P38 and M14 - STACK's'_PURGE_VALVE_Afb_0A001

Current monitoring (STACK's'_PURGE_VALVE_Afb_0A001) for each stack purge valve.

4.4.4.3.6.6 P39 and M12 - STACK's'_PURGE_POS's'_DHI_V

Measurement of the purge valve position feedback switch converted to an internal parameter (STACK's'_PURGE_POS's'_DHI_V).

4.4.4.3.6.7 P43 and M16 - DILUTION_FAN_FI_1HZ

Measurement of the dilution fan speed and conversion to an internal parameter (DILUTION_FAN_FI_1HZ) for diagnostic purposes.

4.4.4.3.6.8 P44 and D10 - H2_AI_0PC1

THE CAN data received from the hydrogen sensor to use as the hydrogen percentage (H2_AI_0PC1) parameter.

4.4.4.3.7 Stack control Internals (STACK_ CONTROL)

4.4.4.3.7.1 P31 - H2_VALVE_PWM_DP

The control parameter for the hydrogen valve PWM demand. Closely related to the fuel cell state machine to determine the operational requirements for the hydrogen valve.

4.4.4.3.7.2 P56 - SAFE_DP

The safety output from the watchdog. If the monitor (PCc_WDOG) determines that the microcontroller is not working correctly or the software detects a serious malfunction (FCS_FAULT_DP) and requires shutting down of the system (in an uncontrolled way i.e.no warning to the vehicle driver) the SAFE_DP parameter is set which will drop out the external control valves forcing the system to shut down into a safe state.

4.4.4.3.7.3 P30 - FCS_FAULT_DP

Set when the software (generally through PCcs) determines that the system is malfunctioning and wishes to initiate an uncontrolled shutdown of the system. If control can still be maintained (even at reduced power) or the fault is not serious then normally the FCCS would shut down in a controlled manner.

4.4.4.3.7.4 P35 - STACK's'_PURGE_VALVE_DEMAND_DP

The control demand for the purge valve for each stack (1 to 's').

4.4.4.3.7.5 P67 - STACK's'_PURGE_HEAT_DEMAND_DP

The control demand for the purge valve heaters for each stack (1 to 's').

4.4.4.3.7.6 P41 - DILUTION_FAN_DEMAND_DP

The control demand for the dilution fan.

4.4.4.3.8 Stack control Outputs (STACK_ CONTROL)

4.4.4.3.8.1 P32 and O10 - H2_VALVE_PO_0PC1

The H2_VALVE_PO_0PC1 signal controls the opening of the H2 valve.

4.4.4.3.8.2 P56 - SAFE_DP and O11 - H2_VALVE_SO_0V

The H2_VALVE_SO_0V switches the 0V to the hydrogen valve based on the safety signal (SAFE_DP). This provides a second method for closing the valve should the H2_VALVE_PO_0PC1 (4.4.4.3.1.1) fail.

4.4.4.3.8.3 P36 and O12 - STACK's'_PURGE_VALVE_DHO_V

Based on the purge valve demand derived from the FCCS state machine, the purge valve will periodically be requested to open for a pre-determined period.

4.4.4.3.8.4 P56 - SAFE_DP and O13 - PURGE_VALVES_SO_0V

The redundant path to close the purge valve if required.

4.4.4.3.8.5 P68 and O14 - STACK's'_PURGE_HEAT's'_DHO_V

Based on ambient temperatures this purge valve heater for each stack (1 to 's') will be controlled based on temperature and operating conditions.

4.4.4.3.8.6 P56 - SAFE_DP and O15 - PURGE_HEAT_SO_0V

The redundant path to turn off the purge valve heater if required.

4.4.4.3.8.7 P30 and O19 - DILUTION_FAN_SO_0V

The redundant path to turn off the dilution fan if required.

4.4.4.3.8.8 P42 and O16 - DILUTION_FAN_PO_0PC1

The speed control for the dilution fan based on the FCCS state machine and hydrogen concentrations assumed and measured in the exhaust i.e. purge control will normally pre-trigger increased dilution fan speed.

4.4.4.4 *High Voltage Interlock (HVIL) and Isolation Testing Classified Signals*

The HVIL and Isolation Testing signals and elements are shown in Figure 36

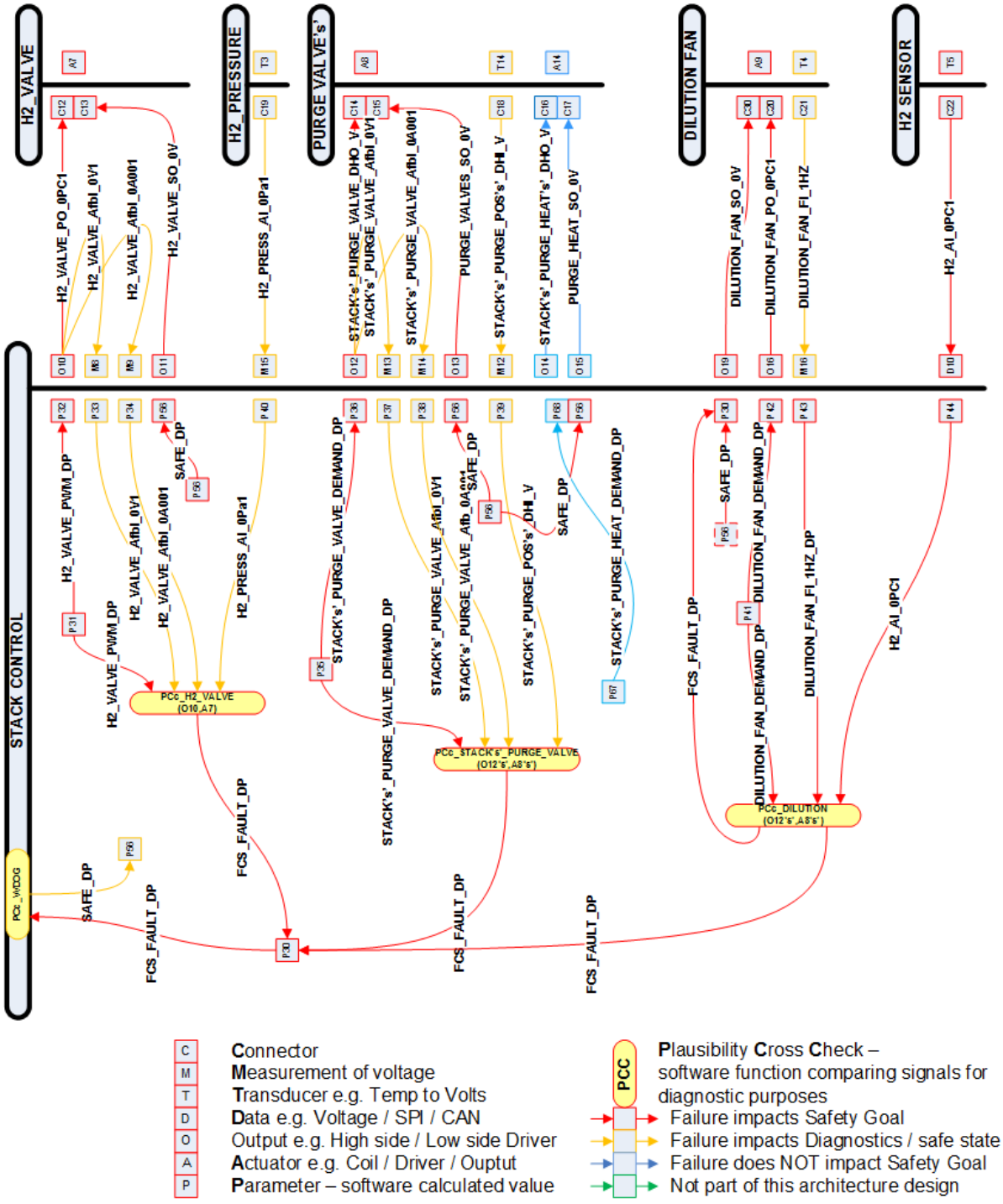


Figure 36: HVIL and Isolation Testing Signals and Elements

4.4.4.4.1 Stack Control Internals (STACK CONTROL)

4.4.4.4.1.1 P16 - ISOT_ST_TIMER_DP

To run the self-test an internal timer is required to trigger the test. This is set by the parameter ISOT_ST_TIMER_DP.

4.4.4.4.2 Stack Control Outputs (STACK CONTROL)

4.4.4.4.2.1 P8, P13 - - STACK's'_HVIL_TRIP_DP and O1 - HVNEG_DHO_V

If an internal trip occurs that requires that the high voltage output to disconnect, parameter STACK's'_HVIL_TRIP_DP will be set which will disable the output HVNEG_DHO_V.

4.4.4.4.2.2 P14 - ISOL_TEST_DHO_V_DP and O5 - ISOL_TEST_DHO_V

The isolation self-test will wait for a time trigger and then request a self-test of the isolation monitoring system via the parameter ISOL_TEST_DHO_V_DP and which drives the output ISOL_TEST_DHO_V.

4.4.4.4.2.3 O3 - HVIL_OUT_DHO_V_DP and A15 - HVIL_OUT_AO_0V01

The HVIL system is driven by the stack controller. The circuit is enabled on by the output HVIL_OUT_DHO_V_DP which drives an actuator which is current controlled output (HVIL_OUT_AO_0V01) to improve diagnostic capability.

4.4.4.4.2.4 P53 - ISOT_AI_1KR_DP and D27 - FCS_1KR_DP_TX

The Isolation Tester provides an input to the stack controller (4.4.4.4.3.1), if the PCC_Isot_ST is satisfied then this value is converted to parameter ISOT_AI_1KR_DP ready to be output over CAN (FCS_1KR_DP_TX).

4.4.4.4.3 Stack Control Inputs (STACK CONTROL)

4.4.4.4.3.1 M5 and P15 - ISOT_AI_1KR

The measurement of the isolation value. Various isolation monitoring systems exist but for this study a voltage input is assumed as per the design discussed in section 4.2. This is converted to a scaled resistance value (ISOT_AI_1KR).

4.4.4.4.3.2 M26 and P9 - HVIL_OUT_AfbI_0V01

As the HVIL circuit is current controlled a known voltage can be monitored (M26) back into the stack controller for diagnostic purposes (HVIL_OUT_AfbI_0V01).

4.4.4.4.3.3 M27 and P10 - HVIL_MID_AI_0V01

The high voltage interlock system has the possibility to diagnose which stack (1 to 's') has tripped. In this application with two stacks in series ('s' = 2) then one HVIL_MID_AI_0V01 voltage feedback is required to determine which stack has an interlock problem.

4.4.4.4.3.4 M28 and P11 - HVIL_IN_AI_0V01

The return HVIL voltage is monitored (M28) and converted to a voltage parameter (HVIL_IN_AI_0V01) and used to determine if the HVIL has tripped and if so, where in the high voltage output circuit this has occurred.

4.4.4.4.3.5 M29 and P12 - HVIL_OK_HDI_V

Rather than rely on software processing entirely for the HVIL circuit and additional window comparator with a delay is used (M29) to generate a digital input parameter (HVIL_OK_HDI_V) that can be additionally be used for diagnostics.

4.4.4.4.4 High Voltage Control (HV CONTROL)

4.4.4.4.4.1 A11 - ISOL_TEST_DHO_V

This is classed as an actuator as it is via an opto-isolator to ensure electrical isolation between the HV system and the low voltage control system.

4.4.4.4.5 Isolation Teser (ISOLATION)

4.4.4.4.5.1 04 - ISOT_AI_1KR

The output from the isolation monitoring system used to pass the isolation resistance value (ISOT_AI_1KR) to the Stack Control system. Note: T4 is considered outside of the scope of this item as it is an independent standalone unit as discussed in section 4.2.

4.4.4.4.6 High Voltage DCDC Converter (DCDC)

4.4.4.4.6.1 C32 - HVNEG_AO_V

Input connection to the DCDC converter for the high voltage negative rail.

4.4.4.4.6.2 C31 - HVPOS_AO_V

Input connection to the DCDC converter for the high voltage positive rail.

4.4.4.4.6.3 C33 - HVIL_OUT_AO_0V01

Connection out to the DCDC converter for the HVIL.

4.4.4.4.6.4 C34 - HVIL_MID_AI_0V01

Mid-point connection (between stack 1 and stack 2 for the HVIL.

4.4.4.4.6.5 C35 - HVIL_IN_AI_0V01

Return connection for the HVIL.

4.4.4.4.7 Hybrid Control (HYBRID CONTROL)

4.4.4.4.7.1 D28 - FCS_1KR_DP_TX

The isolation resistance measurement for the FCCS. Note this includes the input side to the DCDC converter once the HV contactors have closed.

4.4.4.5 Control Parameters and Data Classified Signals

Figure 37 shows the Control Parameters.

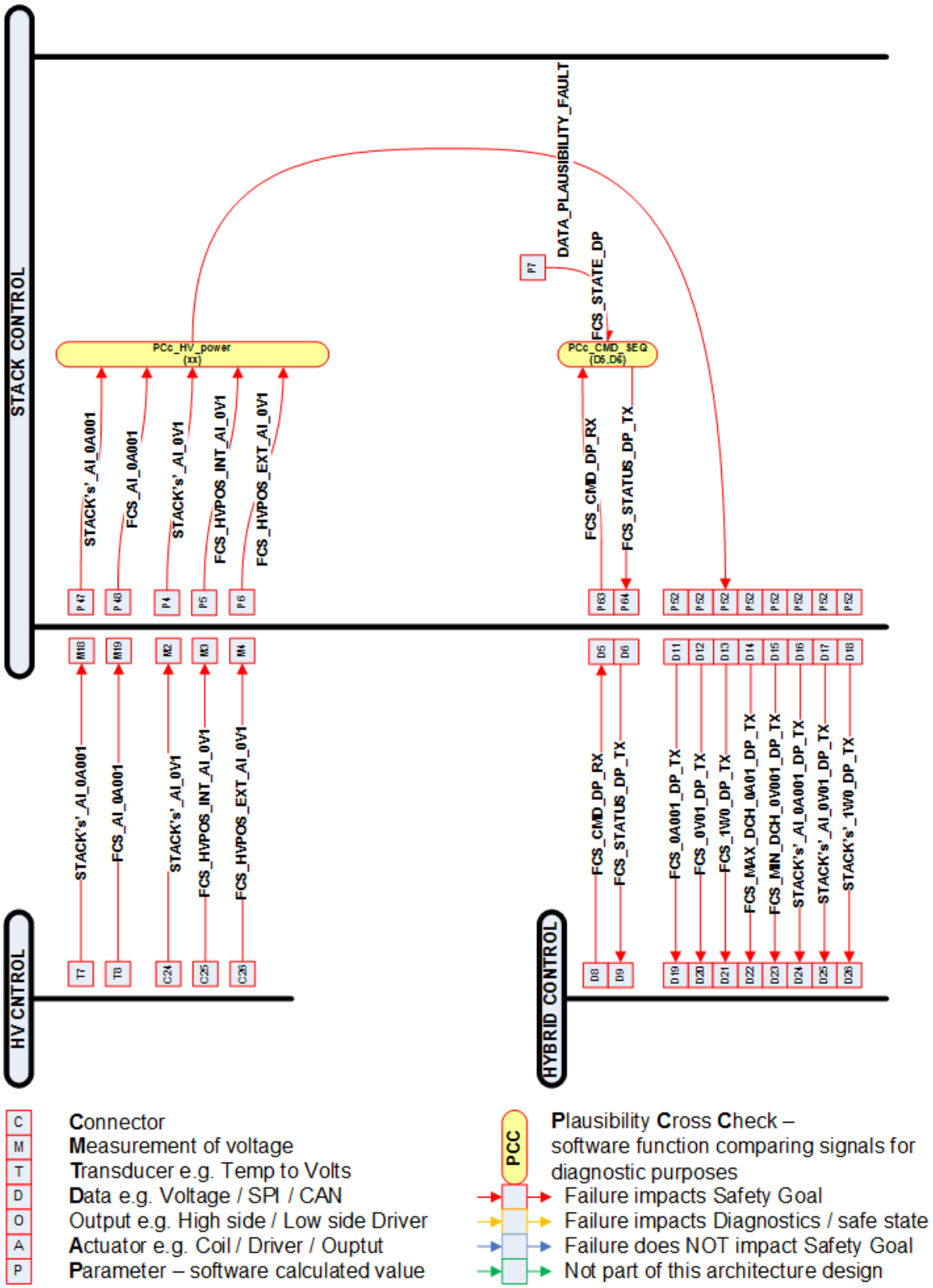


Figure 37: Control Parameters and Data

4.4.4.5.1 Stack Control Inputs (STACK CONTROL)

4.4.4.5.1.1 D5 and P63 - FCS_CMD_DP_RX

The data received from the Hybrid Control unit. This sets requirements to start up, deliver power and shut down etc. thus allowing the FCS to react to demands.

4.4.4.5.2 Stack Control Outputs (STACK CONTROL)

4.4.4.5.2.1 P64 and D6 - FCS_STATUS_DP_RX

The internal parameter for the FCS status. This is based on the main FCCS state machine covering power up self-tests, start-up states, contactor status, running mode and shutdown states etc. This continually informs the hybrid controller about the FCCS state so that it can make decisions. For example, once it knows the contactors are closed it can increase load to the DCDC converter based on additional control parameters discussed in this section.

4.4.4.5.2.2 P52 - DATA_PLAUSIBILITY_FAULT_DP

Any error in data reception / transmission generates parameters that indicate the status of the relevant data parameter. Including all of these parameters in this concept design would significantly increase complexity (and violate the aim of the concept analysis). Instead, a single parameter is used which supports all of the diagnostic techniques applied to the data; this is sufficient for the concept analysis and also elicits requirements for the subsequent system design.

4.4.4.5.2.3 D11 - FCS_0A001_DP_TX

The actual output current drawn from the FCS and delivered to the DCDC converter. This does not include any parasitic losses within the FCCS.

4.4.4.5.2.4 D12 - FCS_0V01_DP_TX

The actual output voltage of the FCS, i.e. the voltage expected at the input to the DCDC converter assuming no voltage drop in the cables that interconnect the two systems.

4.4.4.5.2.5 D13 - FCS_1W0_DP_TX

The power of the complete FCS. This includes any parasitic losses in the FCCS. If the hybrid control system requires an output power value, it can use the current and voltage signals discussed previously.

4.4.4.5.2.6 D14 - FCS_MAX_DCH_0A01_DP_TX

The maximum discharge current that can be drawn from the FCS. The hybrid controller should obey this limit for full control to be maintained. If, for any reason, the FCS needs to de-rate or wishes to open contactors (i.e. reduce switching current of the contactors) then it can communicate this to the hybrid controller.

4.4.4.5.2.7 D15 - FCS_MIN_DCH_0V001_DP_TX

In some instances, the hybrid controller may choose to ignore the maximum discharge current limit, in which case it may draw more current but should still obey the minimum voltage limit for discharge.

4.4.4.5.2.8 D16 - STACK's'_AI_0A001_DP_TX

The current for each stack (1 to 's'). Normally with series connected stacks this current will be identical, however in some cases a stack may be switched out of circuit. Having independent signals for each stack allows this operation to be monitored. It also allows additional diagnostics on the data should this be required by the hybrid controller. It is also useful if stacks are wired in parallel – in which case each stack may provide a slightly different current output.

4.4.4.5.2.9 D17 - STACK's'_AI_0V01_DP_TX

The individual stack voltage. As the stacks are typically in series, each stack may have a slightly different output voltage which can be monitored with each stack ('s') voltage signal. If the stacks are configured in parallel then the voltage signals would be identical (within measurement tolerance limits).

4.4.4.5.2.10 D18 - STACK's'_1W0_DP_TX

An individual power rating for each stack based on the individual current and voltage measurements discussed previously.

4.4.4.6 Diagnostic Coverage

Each of the elements are individually referenced and described in this section with the diagnostic coverage achieved by each of the plausibility checks detailed section 4.4.4.7 through to 4.4.4.11. Table 77 acts as a cross reference to the appendices for the associated diagnostic coverage calculations which also detail each PCc used in the calculation.

Table 77: FCCS Element Cross Reference to Diagnostic Coverage Claims

Element	**Diagnostic Coverage Calculation Table Reference in Appendix F – FCCS – Candidate Architecture DC% Claims**
A1	Table 171: FCCS - Actuator 1
A2	Table 172: FCCS - Actuator 2
A3	Table 173: FCCS - Actuator 3
A4	Table 174: FCCS - Actuator 4
A7	Table 175: FCCS - Actuator 7
A8	Table 176: FCCS - Actuator 8

Element	Diagnostic Coverage Calculation Table Reference in Appendix F – FCCS – Candidate Architecture DC% Claims
A9	Table 177: FCCS - Actuator 9
A10	Table 178: FCCS - Actuator 10
A12	Table 179: FCCS - Actuator 12
A13	Table 180: FCCS - Actuator 13
C1	Table 181: FCCS - Connection 1
C4	Table 182: FCCS - Connection 4
C5	Table 183: FCCS - Connection 5
C6	Table 184: FCCS - Connection 6
C7	Table 185: FCCS - Connection 7
C9	Table 186: FCCS - Connection 9
C12	Table 187: FCCS - Connection 12
C13	Table 188: FCCS - Connection 13
C14	Table 189: FCCS - Connection 14
C15	Table 190: FCCS - Connection 15
C20	Table 191: FCCS - Connection 20
C22	Table 192: FCCS - Connection 22
C24	Table 193: FCCS - Connection 24
C25	Refer to C24 as similar techniques used
C26	Table 194: FCCS - Connection 26
C30	Table 195: FCCS - Connection 30
D1, D3 – D38	Table 196: FCCS - Data 1 (subset 1) Table 197: FCCS - Data 1 (subset 2)
M1	Table 198: FCCS - Measurement 1
M2	Table 199: FCCS - Measurement 2
M3	Refer to M2 as similar techniques used
M4	Table 200: FCCS - Measurement 4
M7	Table 201: FCCS - Measurement 7
M18	Table 202: FCCS - Measurement 18
M19	Refer to M18 as similar techniques used
01	Table 203: FCCS - Output 1
02	Table 204: FCCS - Output 2

Element	Diagnostic Coverage Calculation Table Reference in Appendix F – FCCS – Candidate Architecture DC% Claims
06	Table 205: FCCS - Output 6
07	Table 206: FCCS - Output 7
O10	Table 207: FCCS - Output 10
O11	Table 208: FCCS - Output 11
O12	Table 209: FCCS - Output 12
O13	Table 210: FCCS - Output 13
O16	Table 211: FCCS - Output 16
O17	Table 212: FCCS - Output 17
O19	Table 213: FCCS - Output 19
P7	Table 214: FCCS - Parameter 7 (subset 1) Table 215: FCCS - Parameter 7 (subset 2) Table 216: FCCS - Parameter 7 (subset 3)
P57	Table 217: FCCS - Parameter 57 (subset 1) Table 218: FCCS - Parameter 57 (subset 2) Table 219: FCCS - Parameter 57 (subset 3)
PSU	Table 220: FCCS - PSU
T2	Table 221: FCCS - Transducer 2
T5	Table 222: FCCS - Transducer 5
T7	Table 223: FCCS - Transducer 7
T8	Table 224: FCCS - Transducer 8

Note – not all element references are used as some element references were assigned and then not used as the development of the FCCS proof of concept design progressed. Re-allocation of obsolete references was avoided throughout the project for clarity.

4.4.4.6.1 Element '1)A1'

The negative contactor is monitored by PCc_HVHEG (4.4.4.7.5) to ensure correct opening and closing by online feedback and PCc_PSU_Mon (4.2.5.4.4) to ensure that the power supply to the actuator is within limits.

4.4.4.6.2 Element '1)A2'

The positive contactor is monitored by PCc_HVPOS (4.4.4.7.6) to ensure correct opening and closing by online feedback and PCc_PSU_Mon (4.2.5.4.3) to ensure that the power supply to the actuator is within limits.

4.4.4.6.3 Element '1)A3'

Limited coverage is given by PCc_FAN's'_SPEED (4.4.4.8.4). PCc_FAN's'_POWER (4.4.4.8.3) is not used in this case as only the output is monitored not the actual load. This element can be further analysed by a detailed FMEA to provide a more detailed model that may allow the PCc claim to be increased. For example, understanding failure modes in the fan as the control signals tend to indicate an internal power supply control and speed control circuit.

4.4.4.6.4 Element '1)A4'

The claim is increased for the PWM output as this is directly related to the feedback signal which can monitor the change in PWM directly by PCc_FAN's'_SPEED (4.4.4.8.4) and a known transfer function applied.

4.4.4.6.5 Element '1)A7'

Diagnostic coverage on the hydrogen valve is high due to PCc_H2_VALVE (4.4.4.9.1).

4.4.4.6.6 Element '1)A8'

PCc_STACK's'_PURGE_VALVE (4.4.4.9.2) provides relatively good diagnostics, however, there are concerns that a single digital input, although an independent monitor, does not give a true analogue feedback over the mechanical range of the valve. This may limit the accuracy of detection and allow incorrect indication of fully open (which may prove not to be an issue) or fully closed (which may lead to a slow release of hydrogen into the exhaust system).

4.4.4.6.7 Element '1)A9'

PCc_DILUTION (4.4.4.9.3) provides good diagnostics based on the fact that the fan is rotating, however there are questions regarding the ability of the hydrogen sensor measuring a true representation of hydrogen in the exhaust due to mixing of gases. Further examination of a proposed application may allow this coverage to be increased. Also, the sensor is expensive and so its ability to improve safety would have to be justified against its cost with an ALARP study.

4.4.4.6.8 Element '1)A10'

High diagnostics are achieved on the pre-charge due to the simplicity of the voltage measurements PCc_PSU_Mon (4.2.5.4.4) for the power supply and PCc_PRECHG (4.4.4.7.2) for the actual pre charge output, the independence of channels and the fact that a number of the measurements can be verified by external systems e.g. the DCDC converter and individual cell monitoring.

4.4.4.6.9 Element '1)A12'

As the inlet damper is part of a temperature control loop and the position monitor, not part of the closed loop control it provides a reliable independent method of proving position by

PCc_INLET's'_POSITION (4.4.4.8.1). In the initial concept there are questions about positional accuracy and the mechanical linkage between the feedback monitoring point and the actual damper position as some failure may potentially have limited coverage.

4.4.4.6.10 Element '1)A13'

As the exhaust damper is part of a temperature control loop and the position monitor, not part of the closed loop control it provides a good independent method of proving position by PCc_EXHAUST's'_POSITION (4.4.4.8.2). As above, there are questions about positional accuracy and the mechanical linkage between the feedback monitoring point and the actual damper position as some failures may potentially have limited coverage.

4.4.4.6.11 Element '1)C1'

Coverage of 48% is achieved by PCc_OA_WINDOW (4.4.4.7.1). To increase coverage further work is required on the design in order to prove the connections to the cells and any interference / drift that can result. It is likely that this estimate is conservative and coverage can be increased following a more detailed investigation.

4.4.4.6.12 Element '1)C4'

Improvement on diagnostic coverage would require additional requirements to be placed on the DCDC converter. As this is not confirmed at this stage no claim is made even though PCc_HVNEG (4.4.4.7.5) is used. As part of a production intent design, requirements can be placed on the DCDC converter manufacturer to provide qualified independent feedback that would prove the final connection.

4.4.4.6.13 Element '1)C5'

Discussion as per Element '1)C4' 4.4.4.6.12 apart from PCc_HVPOS (4.4.4.7.6) is used.

4.4.4.6.14 Element '1)C6'

PCc_FAN's'_POWER (4.4.4.8.3) gives high coverage of the harness up to the connector input due to the monitoring feedback provided on the output driver.

4.4.4.6.15 Element '1)C7'

The connection is directly related to the feedback signal which can monitor the change in PWM directly by PCc_FAN's'_SPEED (4.4.4.8.4).

4.4.4.6.16 Element '1)C9'

Relatively high diagnostics are achieved by knowing the characteristics of the thermocouple used and the fact that this can be verified within a tolerance by independent sensors using PCc_STACK's'_TEMP (4.4.4.8.5).

4.4.4.6.17 Element '1)C12'

Relatively low diagnostics are achieved by having limited characteristic knowledge of the hydrogen valve when controlled with a PWM signal. Further investigation may improve the diagnostic claim from that initially claimed by PCc_H2_VALVE (4.4.4.9.1).

4.4.4.6.18 Element '1)C13'

See discussion 4.4.4.6.17. Further analysis of the valve is required to understand the ground connection with reference to the body of the valve before relying on short circuit detection.

4.4.4.6.19 Element '1)C14'

A conservative claim for PCc_STACK's'_PURGE_VALVE (4.4.4.9.2) failure mode coverage is made until full temperature characteristics and voltage / current characteristics are known for the purge valve.

4.4.4.6.20 Element '1)C15'

See dicussion4.4.4.6.19.

4.4.4.6.21 Element '1)C20'

A conservative claim is made using PCc_DILUTION (4.4.4.9.3) until the dilution fan control circuit is understood. Basic diagnostics can be covered for the connection and harness by the frequency feedback signal.

4.4.4.6.22 Element '1)C22'

As this connection uses a data signal, the connection can be validated by correct communication with the sensor and monitored by PCc_DILUTION (4.4.4.9.3).

4.4.4.6.23 Element '1)C24', 1)C25

This connection is comprehensively covered by the sequencing of tests and the independent measurement values used in PCc_V_SUM (4.4.4.7.3) and PCc_HV_WINDOW (4.4.4.7.4).

4.4.4.6.24 Element '1)C26'

This connection is comprehensively covered by the sequencing of tests and the independent measurement values used by PCc_HVPOS (4.4.4.7.6).

4.4.4.6.25 Element '1)C30'

See discussion 4.4.4.6.21.

4.4.4.6.26 Element '1)D1'

The SPI connection is robust and includes a number of built in diagnostics techniques as referred to in the Data section (4.2.5.4.1).

4.4.4.6.27 Element '1)D3 to 1)D38'

All of these data elements have exactly the same PCc and hence diagnostic coverage as '1)D1' (4.4.4.6.26) and so are not shown here. In some cases, additional proof may indicate a higher claim for coverage depending on the final protocol implemented.

4.4.4.6.28 Element '1)M1'

Relatively low claims are made using PCc_OA_WINDOW (4.4.4.7.1) until full validation is provided by the manufacturer of the AFE. This is very conservative at this stage.

4.4.4.6.29 Element '1)M2', 1)M3

Independent verification via multiple techniques PCc_V_SUM (4.4.4.7.3) and PCc_HV_WINDOW (4.4.4.7.4) permit a high PCc claim.

4.4.4.6.30 Element '1)M4'

Controlled test sequences and independent verification via PCc_HVPOS (4.4.4.7.6) permit a high PCc claim.

4.4.4.6.31 Element '1)M7'

Insufficient justification is available for claiming diagnostic coverage on this element. It is, however, used a cross check for other temperature measurements. Claiming coverage on this element as well would generate a circular argument and so avoided.

4.4.4.6.32 Element '1)M18', '1)M19'

High coverage is achieved through independent verification using PCc_A_SUM (4.4.4.7.7). If stacks were connected in parallel then diagnostic coverage may be reduced and this should be considered on an application by application basis.

4.4.4.6.33 Element '1)O1'

See discussion 4.4.4.6.1.

4.4.4.6.34 Element '1)O2'

Refer to description for Element '1)A2 (4.4.4.6.2).

4.4.4.6.35 Element '1)O6'

As PCc_FAN's'_POWER (4.4.4.8.3) is used along with PCc_PSU_Mon (4.2.5.4.4), the intelligent high side drive output allows a diagnostic coverage claim of 98 %.

4.4.4.6.36 Element '1)O7'

Refer to discussion on Element '1)A4' (4.4.4.6.4).

4.4.4.6.37 Element '1)O10'

High claim for the actual on-board output driver due to the feedback provided and monitoring by PCc_H2_VALVE (4.4.4.9.1) and power supply monitoring PCc_PSU_Mon (4.2.5.4.4).

4.4.4.6.38 Element '1)O11'

No claim is made for this as it is provided as a safety shutdown. Further investigation may allow a claim to be made based on measurements made for '1)O10' (4.4.4.6.37). The power supply is covered but this still leaves undiagnosed faults that require coverage even for a 60% claim.

4.4.4.6.39 Element '1)O12'

A high claim is made for the actual on-board output driver due to the feedback provided and monitoring by PCc_STACK's'_PURGE_VALVE (4.4.4.9.2) and power supply monitoring PCc_PSU_Mon (4.2.5.4.4).

4.4.4.6.40 Element '1)O13'

No claim is made for this as it is provided as a safety shutdown. Further investigation may allow a claim to be made based on measurements made for '1)O12' (4.4.4.6.39). The power supply is covered but this still leaves undiagnosed faults that require coverage even for a 60% claim.

4.4.4.6.41 Element '1)O16'

High coverage is achieved on the speed control due to the frequency feedback and monitoring (PCc_DILUTION (4.4.4.9.3)) and power supply monitoring (PCc_PSU_Mon (4.2.5.4.4)) for the output driver.

4.4.4.6.42 Element '1)O17'

See discussion on Element '1)A10' (4.4.4.6.8.)

4.4.4.6.43 Element '1)O19'

No claim is made as there is no specific feedback on the output itself. Further study may show a characteristic between speed (which is monitored) and failures on the output itself but this is not understood sufficiently at this stage relating to the 0V connection and the failure modes detectable by the intelligent output driver.

4.4.4.6.44 Element '1)P7', 1)P57

A high claim is made due to on-board diagnostics for random access memory available in the microcontroller (4.2.5.4.3). This would need to be verified to ensure that all the available techniques assumed are actually run as part of the monitoring sequences.

4.4.4.6.45 Element '1)PSU'

The power supply, in this case, is a companion chip for the microcontroller and so provides high coverage on both supply rails and internal reference voltages. These are available as both digital signals over SPI and as analogue voltages through a multiplexer. This facilitates other tests on analogue inputs. It also contains a question and answer watchdog to ensure correct microcontroller operation. Full details are available from manufacturers once NDA's are in place.

4.4.4.6.46 Element '1)T2'

See discussion on Element '1)M7' (4.4.4.6.31).

4.4.4.6.47 Element '1)T5'

There is very limited coverage on the Hydrogen sensor at present. There is an argument just to use it for diagnostics only but also some questions around using it for control of H2 and purge to monitor concentration. For that reason, no claim is currently made.

4.4.4.6.48 Element '1)T7', '1)T8'

See discussion on Element '1)M18)' (4.4.4.6.32).

4.4.4.7 Voltage and Current Based Measurement and Control Plausibility Cross-checks

A number of PCcs are used in the voltage and current measurement control system. These are discussed in the following sections.

4.4.4.7.1 PCc_OA_Window / PCc_OA_TRIP

The operating window uses one main function which ensures each of the individual cell voltages are within voltage limits and temperate limits. This includes an upper and a lower limit. In order to increase diagnostic coverage a number of internal self-tests are continually run in the AFE at the request of the Stack Control microcontroller.

The internal tests are typically:

- Under Voltage comparison – a flag set in the AFE against pre-programmed threshold.
- Over Voltage comparison – a flag set in the AFE against pre-programmed threshold.
- Sum of cells – a sum of cells measurement request made over isoSPI.

- ADSTATcommand –measures sum of cells (above), internal die temperature and 5V power supply.
- ADAX command –measures the second reference voltage.
- DIAGN command –triggers a multiplexer decoder check.
- CVST command –triggers a cell voltage conversion and poll check.
- AXST command –triggers a general-purpose input / output conversion and poll status check.
- STATST command – triggers a self-test status group conversion and poll status.
- ADOW command – triggers an open wire analog to digital convertor (ADC) conversion and poll status check.

The Stack Control microcontroller sequences through these comprehensive self-tests on a regular basis to ensure that the diagnostic tests are performed repeatedly and that results are valid.

4.4.4.7.2 PCc_PRECHG

To ensure that a pre-charge is completed correctly, a controlled (current limited) output charges any DCDC converter load capacitance. This allows a number of diagnostics to be performed. The internal FCS voltage is known (FCS_HVPOS_INT_AI_0V1) so by providing a known current output into a known load it is possible to monitor the output voltage (FCS_HVPOS_INT_AI_0V1) to determine the output voltage profile with respect to time. This allows the output voltage measurement circuitry to be checked as the voltage rises and a comparison made between input and output measurements in a controlled way before any significant current is made available at the output.

4.4.4.7.3 PCc_V_SUM

The internally measured voltage (FCS_HVPOS_INT_AI_0V1) at the Stack Control output can be compared against the individual stack voltages (STACK's'_AI_0V01). In this application, there are two stacks, in other applications a higher multiple of stacks can be linked in series.

4.4.4.7.4 PCc_HV_Window

The internally measured voltage (FCS_HVPOS_INT_AI_0V1) at the Stack Control output can be compared against the stack voltage measured at the Cell Control system. These use independent measurement circuits giving a high confidence level. This can be further improved by looking at the individual stack voltages (STACK's'_AI_0V01).

4.4.4.7.5 PCc_HV_NEG

By suitable placement of the measurement points, it is possible to examine faults on the negative contactor prior to closing the positive contactor.

4.4.4.7.6 PCc_HV_POS

By suitable placement of the measurement points it is possible to examine faults on the positive contactor prior to opening the negative contactor and after the negative contactor has closed. The main aim with the contactor checks is to ensure that prior to closing the contactors, there are two independent means to open the contactors. During a drive cycle it is possible that one of these may fail but sufficiently unlikely that both will fail within the drive cycle and so at least one route always remains to disconnect the high voltage if required.

4.4.4.7.7 PCc_A_SUM

The internally measured current (FCS_AI_0A001) at the Stack Control output can be compared against the individual stack currents (STACK's'_AI_0A001). In this application there are two stacks, in other applications a higher multiple of stacks could be linked in series. As the stacks are in series, the current will be the same for each stack. In some applications a single stack may be shut down and the suggested route to measure current still provides a plausibility check between the individual stack current and the overall FCS current.

4.4.4.8 Air Flow and Temperature Control Plausibility Cross-checks.

A number of PCcs are used in the air flow and temperature control system. These are discussed in the following sections.

4.4.4.8.1 PCc_INLET's'_POSITION

PCc between the demand for the inlet damper position and the feedback. As well as running periodic tests this can also be verified during start up or shut down to confirm end points for open and close position, rates of change of position and the characteristic curve of the damper opening which achieves high diagnostic coverage.

4.4.4.8.2 PCc_OUTLET's'_POSITION / PCc_EXHAUST's'_POSITION

PCc between the demand for the outlet damper position and the feedback. Similar principles are used to that of the inlet fan diagnostics (4.4.4.8.1).

4.4.4.8.3 PCc_FAN's'_POWER

PCc that looks at the fan control power requirements based on the fan state machine and monitors power to each of the stack (1 to 's') fans (1 to 'f') to ensure correct power curves. For a specific speed demand, at a measured voltage, the current is validated to be within a specific target range for given inlet and outlet damper combinations.

4.4.4.8.4 PCc_FAN's'_SPEED

PCc that looks at the fan control speed requirements based on the fan state machine and monitors actual speed against demand for each of the stack (1 to 's') fans (1 to 'f') to ensure a correct speed tolerance. This is further enhanced by monitoring cathode air pressure. Additionally, cathode air pressure can be used to monitor filter particulate accumulation but this is not considered a safety feature for power control as it would provide a gradual increase in pressure drop which is monitored and controlled through maintenance.

4.4.4.8.5 PCc_Stack's'_Temp

PCc that monitors pressure, fan speed and temperature to ensure that all the parameters correlate within a window and that changes in control demand parameters have correct results measured by the feedback signals. This is quite a complex monitoring function and in a final solution may be broken down into a number of subsystems. However, at this stage, analysing the concept it was considered acceptable.

4.4.4.9 Hydrogen Delivery Control, Dilution and Purging Plausibility Cross-checks.

Many PCcs are used in the hydrogen control system. These are discussed in the following sections.

4.4.4.9.1 PCc_H2_VALVE

The power to the hydrogen valve is monitored to detect faults in the coil or abnormal operating conditions. The current feedback is also used to maintain holding current based on voltage for the hydrogen valve to minimise parasitic power.

Additional monitoring is provided by the hydrogen pressure sensor both in terms of the hydrogen valve and upstream mechanical pressure regulation.

4.4.4.9.2 PCc_STACK's'_PURGE_VALVE

Voltage and current feedback is used to detect failures in the electrical side of the purge valve. Additional feedback is provided from a feedback signal in the valve that indicates whether the valve has opened when requested.

4.4.4.9.3 PCc_DILUTION

The dilution fan speed is monitored to ensure that the demand for fan speed is acted upon and that the fan has not stalled or is electrically open circuit. Additional feedback is provided by the hydrogen sensor although this is purely a secondary check on the overall hydrogen control system.

4.4.4.10 High Voltage Interlock (HVIL) and Isolation Testing Plausibility Cross-checks.

A number of PCcs are used in the hydrogen control system. These are discussed in the following sections.

4.4.4.10.1 PCc_HVIL_TRIP

This PCc purely monitors software status STACK's'_HVIL_SW_TRIP_DP against the hardware status to provide a software controlled shutdown prior to a hardware shutdown as provided by the hardware system (HVIL_OK_V_HSDI).

4.4.4.10.2 PCc_ISOT_ST

Providing an independent asynchronous self-test function for the isolation monitoring is a cross check that was developed in 4.2 and is carried over into this proof of concept.

4.4.4.10.3 PCc_HVIL_ST

The HVIL self-test is comprehensive. It allows test at power up, power on and continual monitoring for latent faults during runtime.

4.4.4.11 Control Parameters and Data Plausibility Cross Checks

The PCcs are covered in the sections on Data (4.2.5.4.1) and Parameters (4.2.5.4.3).

4.4.5 Overall Analysis

4.4.5.1 Maintain Power within Operating Area –Analysis

The architectural metrics are calculated as discussed in 3.7.2, with the SPFM calculation shown in Table 78 and the LFM calculation shown in Table 79.

Table 78: FCCS Maintain Power SPFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Distributed Failure Rate	Failure mode that has the potential to violate the SG in the absence of a Safety Mechanism	PCc applicable to prevent violation of Safety Goal	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
HV CONTROL Inputs											
STACK's'_AI_0V1	Connection	1)C24	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y	PCc_V_SUM, PCc_HV_WINDOW	99%	1.4E-04
FCS_HVPOS_INT_AI_0V1	Connection	1)C25	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y	PCc_V_SUM, PCc_HV_WINDOW	99%	1.4E-04
FCS_HVPOS_EXT_AI_0V1	Connection	1)C26	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y	PCc_HVPOS	99%	1.4E-04
STACK's'_AI_0A001	Transducer	1)T7	4.0E+01	Y	4.0E+01	40%	1.6E+01	Y	PCc_A_SUM, PCc_PSU_MON	98%	3.9E-01
FCS_AI_0A001	Transducer	1)T8	4.0E+01	Y	4.0E+01	40%	1.6E+01	Y	PCc_A_SUM, PCc_PSU_MON	98%	3.9E-01
HV CONTROL Internals											
HVNEG_DHO_V	Actuator	1)A1	3.0E+01	Y	3.0E+01	40%	1.2E+01	Y	PCc_HVNEG, PCc_PSU_MON	72%	3.4E+00
HVPOS_PRECHG_HDO_V	Actuator	1)A10	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y	PCc_PRECHG, PCc_PSU_MON	99%	5.5E-02
HVPOS_HDO_V	Actuator	1)A2	1.9E+02	Y	1.9E+02	40%	7.7E+01	Y	PCc_HVPOS, PCc_PSU_MON	72%	2.2E+01
HV CONTROL Outputs											
HVNEG_AO_V	Connection	1)C4	3.0E+00	Y	3.0E+00	40%	1.2E+00	Y	PCc_HVNEG	0%	1.2E+00
HVPOS_AO_V	Connection	1)C5	3.0E+00	Y	3.0E+00	40%	1.2E+00	Y	PCc_HVPOS	0%	1.2E+00

STACK CONTROL Inputs

STACK's'_AI_0V1	Measurement	1)M2	4.0E+00	Y	4.0E+00	40%	1.6E+00	Y	PCc_V_SUM, PCc_HV_WINDOW	98%	3.2E-02
FCS_HVPOS_INT_AI_0V1	Measurement	1)M3	6.0E+00	Y	6.0E+00	40%	2.4E+00	Y	PCc_V_SUM, PCc_HV_WINDOW	98%	4.8E-02
FCS_HVPOS_EXT_AI_0V1	Measurement	1)M4	6.0E+00	Y	6.0E+00	40%	2.4E+00	Y	PCc_HVPOS	98%	4.8E-02
STACK's'_AI_0A001	Measurement	1)M18	6.0E+00	Y	6.0E+00	40%	2.4E+00	Y	PCc_A_SUM	98%	4.8E-02
FCS_AI_0A001	Measurement	1)M19	4.0E+00	Y	4.0E+00	40%	1.6E+00	Y	PCc_A_SUM	98%	3.2E-02
CELL'c'_AI_0V0001	Data	1)D3	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
STACK's'_AI_0V001	Data	1)D4	8.3E-01	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_AI_0C1	Data	1)D29	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
FCS_AIR_IN_POS_AI_1Dg	Data	1)D39	8.3E-01	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_EXHAUST_POS_AI_1Dg	Data	1)D40	8.3E-01	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_FAN'f'_FI_HZ	Measurement	1)M6	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_TEMP't'_AI_0C1	Measurement	1)M7	4.0E+00	Y	4.0E+00	40%	1.6E+00	Y	?only really have a range check which is insufficient	0%	1.6E+00
CATHODE_AIR_AI_0Pa1	Measurement	1)M17	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
H2_VALVE_AfbI_0V1	Measurement	1)M8	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
H2_VALVE_AfbI_0A001	Measurement	1)M9	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
H2_PRESS_AI_0Pa1	Measurement	1)M15	4.0E+0	DS	0.0E+0	40%	0.0E+0		Assume for initial analysis that this is	0%	

			0		0		0		just used for diagnostics		
STACK's'_PURGE_VALVE_AfbI_0V1	Measurement	1)M13	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_PURGE_VALVE_AfbI_0A001	Measurement	1)M14	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_PURGE_POS's'_DHI_V	Measurement	1)M12	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
DILUTION_FAN_FI_1HZ	Measurement	1)M16	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
H2_AI_0PC1	Data	1)D10	8.3E-01	DS	0.0E+00	40%	0.0E+00			0%	
FCS_CMD_DP_RX	Data	1)D5	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
STACK's'_FAN'f'_AfbI_0V1	Measurement	1)M21	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_FAN'f'_AfbI_0A1	Measurement	1)M22	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	

STACK CONTROL Internals

SAFE_DP	Parameter	1)P56	1.6E-01	DS	0.0E+00	40%	0.0E+00		Assume for initial analysis that this is just used for diagnostics	0%	
FCS_STATE_DP	Parameter	1)P7	1.6E-01	Y	1.6E-01	40%	6.6E-02	Y	PCc_PSU, PCc_RAM_TEST, PCc_MICRO_TEST	97%	1.6E-03
CAL_WINDOW_DP_0V001	Parameter	1)P57	2.1E-02	Y	2.1E-02	40%	8.3E-03	Y	PCc_PSU, PCc_RAM_TEST, PCc_MICRO_TEST	98%	2.0E-04

STACK CONTROL Outputs

HVNEG_DHO_V	Output	1)O1	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y	PCc_HVNEG, PCc_PSU	98%	8.7E-02
HVPOS_DHO_V	Output	1)O2	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y	PCc_HVPOS, PCc_PSU	98%	8.7E-02

HVPOS_PRECHG_DHO_V	Output	1)O17	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y	PCc_PRECHG, PCc_PSU	98%	8.7E-02
FCS_AIR_IN_PO_0PC1	Data	1)D37	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_EXHAUST's'_POSITION, PCc_DATA_CHECK, PCc_POLL_RESPONSE	97%	1.1E-02
STACK's'_EXHAUST_PO_0PC1	Data	1)D38	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_EXHAUST's'_POSITION, PCc_DATA_CHECK, PCc_POLL_RESPONSE	97%	1.1E-02
STACK's'_FAN'f'_DHO_V	Output	1)O6	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y	PCc_FAN's'_POWER, PCc_PSU	98%	8.7E-02
STACK's'_FAN'f_PO_0PC1	Output	1)O7	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y	PCc_FAN's'_SPEED, PCc_PSU	98%	8.7E-02
H2_VALVE_PO_0PC1	Output	1)O10	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y	PCc_H2_VALVE, PCc_PSU	98%	8.7E-02
H2_VALVE_SO_0V	Output	1)O11	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y		0%	4.8E+00
STACK's'_PURGE_VALVE_DHO_V	Output	1)O12	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y	PCc_STACK's'_PURGE_VALVE, PCc_PSU	98%	8.7E-02
PURGE_VALVES_SO_0V	Output	1)O13	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y		0%	4.8E+00
STACK's'_PURGE_HEAT's'_DHO_V	Output	1)O14	1.2E+01	N	0.0E+00	40%	0.0E+00			0%	
PURGE_HEAT_SO_0V	Output	1)O15	1.2E+01	N	0.0E+00	40%	0.0E+00			0%	
DILUTION_FAN_SO_0V	Output	1)O19	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y		0%	4.8E+00
DILUTION_FAN_PO_0PC1	Output	1)O16	1.2E+01	Y	1.2E+01	40%	4.8E+00	Y	PCc_DILUTION, PCc_PSU	98%	8.7E-02
FCS_0A001_DP_TX	Data	1)D19	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
FCS_0V01_DP_TX	Data	1)D20	8.3E-	Y	8.3E-	40%	3.3E-	Y	PCc_DATA_CHECK, PCc_POLL_RESPONS	91%	3.0E-02

			01		01		01		E		
FCS_1W0_DP_TX	Data	1)D21	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
FCS_MAX_DCH_0A01_DP_TX	Data	1)D22	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
FCS_MIN_DCH_0V001_DP_TX	Data	1)D23	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
STACK's'_AI_0A001_DP_TX	Data	1)D24	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
STACK's'_AI_0V01_DP_TX	Data	1)D25	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
STACK's'_1W0_DP_TX	Data	1)D26	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
FCS_STATUS_DP_TX	Data	1)D6	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02

CELL CONTROL Inputs

CELL'c'_AI_0V0001	Measurement	1)M1	4.0E+00	Y	4.0E+00	40%	1.6E+00	Y	PCc_OA_WINDOW	35%	1.0E+00
STACK's'_AI_0V0001	Measurement	1)M23	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
CELL'c'_AI_0C1	Measurement	1)M20	4.0E+00	DS	0.0E+00	40%	0.0E+00			0%	
CELL'c'_CVL_HSDO	Data	1)D32	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02

CELL CONTROL Outputs

CELL'c'_AI_0V0001	Data	1)D1	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02

STACK's'_AI_0V001	Data	1)D2	8.3E-01	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_AI_0C1	Data	1)D30	8.3E-01	DS	0.0E+00	40%	0.0E+00			0%	

Cell Inputs

CELL'c'_AI_0V0001	Connection	1)C1	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y	PCc_OA_WINDOW	48%	7.3E-03
CELL'c'_AI_0V0001	Connection	1)C2	3.5E-02	DS	0.0E+00	40%	0.0E+00			0%	
CELL'c'_AI_0C1	Connection	1)C3	3.5E-02	DS	0.0E+00	40%	0.0E+00			0%	

Inlet Air Control Inputs

FCS_AIR_IN_PI_0PC1	Data	1)D33	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
FCS_AIR_IN_POS_AI_1Dg	Transducer	1)T10	4.0E+01	DS	0.0E+00	40%	0.0E+00			0%	

Inlet Air Control Outputs

FCS_AIR_IN_PO_0PC1	Actuator	1)A12	8.0E+01	Y	8.0E+01	40%	3.2E+01	Y	PCc_EXHAUST's'_POSITION	71%	9.2E+00
FCS_AIR_IN_POS_AI_1Dg	Data	1)D34	8.3E-01	DS	0.0E+00	40%	0.0E+00			0%	

Exhaust Control Inputs

STACK's'_EXHAUST_PI_0PC1	Data	1)D35	8.3E-01	Y	8.3E-01	40%	3.3E-01	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE	91%	3.0E-02
STACK's'_EXHAUST_POS	Transducer	1)T11	4.0E+01	DS	0.0E+00	40%	0.0E+00			0%	

Exhaust Control Outputs

STACK's'_EXHAUST_PO_0PC1	Actuator	1)A13	8.0E+01	Y	8.0E+01	40%	3.2E+01	Y	PCc_EXHAUST's'_POSITION	71%	9.2E+00
STACK's'_EXHAUST_POS	Data	1)D36	8.3E-01	DS	0.0E+00	40%	0.0E+00			0%	

Stack Fans Inputs

STACK's'_FAN'f'_HSDO	Connection	1)C6	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y		99%	1.4E-04
STACK's'_FAN'f_PWM	Connection	1)C7	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y		99%	1.4E-04
STACK's'_FAN'f'_HZ	Transducer	1)T1	4.0E+01	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_TEMP't'_AI_0C1	Transducer	1)T2	2.0E+00	Y	2.0E+00	40%	8.0E-01	Y	PCc_STACK's'_TEMP	0%	8.0E-01

Stack Fans Outputs

STACK's'_FAN'f'_HSDO	Actuator	1)A3	1.5E+01	Y	1.5E+01	40%	6.0E+00	Y	PCc_FAN's'_SPEED	59%	2.4E+00
STACK's'_FAN'f_PWM	Actuator	1)A4	1.0E+02	Y	1.0E+02	40%	4.0E+01	Y	PCc_FAN's'_SPEED	99%	4.0E-01
STACK's'_FAN'f'_HZ	Connection	1)C8	3.5E-02	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_TEMP't'_AI_0C1	Connection	1)C9	2.0E+00	Y	2.0E+00	40%	8.0E-01	Y	PCc_STACK's'_TEMP	81%	1.5E-01

Cathode Air Pressure Inputs

CATHODE_AIR_AI_0PA1	Transducer	1)T6	4.0E+01	DS	0.0E+00	40%	0.0E+00			0%	

Cathode Air Pressure Outputs

CATHODE_AIR_AI_0PA1	Connection	1)C23	3.5E-02	DS	0.0E+00	40%	0.0E+00			0%	

H2 Valve Inputs

H2_VALVE_PWM	Connection	1)C12	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y	PCc_H2_VALVE	42%	8.2E-03
H2_VALVE_SO_0V	Connection	1)C13	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y	PCc_H2_VALVE	33%	9.5E-03

H2 Valve Outputs

H2_VALVE_PWM	Actuator	1)A7	5.0E+01	Y	5.0E+01	40%	2.0E+01	Y	PCc_H2_VALVE	99%	2.0E-01

H2 Pressure Inputs

H2_PRESS_AI_PA	Transducer	1)T3	4.0E+0	DS	0.0E+0	40%	0.0E+0			0%	

			1		0		0				

H2 Pressure Outputs

H2_PRESS_AI_PA	Connection	1)C19	3.5E-02	DS	0.0E+00	40%	0.0E+00			0%	

Purge Valve Inputs

STACK's'_PURGE_VALVE_HSDO	Connection	1)C14	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y	PCc_STACK's'_PURGE_VALVE	48%	7.3E-03
PURGE_VALVES_SO_0V	Connection	1)C15	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y	PCc_STACK's'_PURGE_VALVE	42%	8.2E-03
STACK's'_PURGE_POS's'_DHI_V	Transducer	1)T14	4.0E+01	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_PURGE_HEAT's'_DHO_V	Connection	1)C16	3.5E-02	N	0.0E+00	40%	0.0E+00			0%	
PURGE_HEAT_SO_0V	Connection	1)C17	3.5E-02	N	0.0E+00	40%	0.0E+00			0%	

Purge Valve Outputs

STACK's'_PURGE_VALVE_DHO_V	Actuator	1)A8	5.0E+01	Y	5.0E+01	40%	2.0E+01	Y	PCc_STACK's'_PURGE_VALVE	71%	5.7E+00
STACK's'_PURGE_POS's'_DHI_V	Connection	1)C18	3.5E-02	DS	0.0E+00	40%	0.0E+00			0%	
STACK's'_PURGE_HEAT's'_DHO_V	Actuator	1)A14	5.0E+01	N	0.0E+00	40%	0.0E+00			0%	

Dilution Fan Inputs

DILUTION_FAN_PO_0PC1	Connection	1)C20	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y	PCc_DILUTION	48%	7.3E-03
DILUTION_FAN_SO_0V	Connection	1)C30	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y	PCc_DILUTION	48%	7.3E-03
DILUTION_FAN_FI_1HZ	Transducer	1)T4	4.0E+01	DS	0.0E+00	40%	0.0E+00			0%	

Dilution Fan Outputs

DILUTION_FAN_FI_HZ	Connection	1)C21	3.5E-02	DS	0.0E+00	40%	0.0E+00			0%	
DILUTION_FAN_PO_0PC1	Actuator	1)A9	1.0E+0	Y	1.0E+0	40%	4.0E+0	Y	PCc_DILUTION	71%	1.2E+01

			2		2		1				

H2 Sensor Inputs

H2_AI_oPC!	Transducer	1)T5	1.0E-02	Y	1.0E-02	40%	4.0E-03	Y		0%	4.0E-03

H2 Sensor Outputs

H2_AI_oPC1	Connection	1)C22	3.5E-02	Y	3.5E-02	40%	1.4E-02	Y		99%	1.4E-04

Isolation tester

Isot (previous calc)	Isot		9.2E+01	Y	9.2E+01	40%	3.7E+01	Y		97%	1.1E+00

High Voltage Interlock

HVIL (estimate)	HVIL		4.0E+01	Y	4.0E+01	40%	1.6E+01	Y		99%	1.6E-01

			1526.8		1113.7						88.1

Single point fault metric	94.2%

Table 79: FCCS Maintain Power LFM Calculation

Signal Description	Element Classification	Element Reference	Failure Rate/FIT	Safety Critical component	Safety Critical Failure rate	Failure rate distribution, %	Multiple Point Failure rate (Perceived + Latent Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %	Distributed Failure Rate	Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent	Failure Mode coverage with respect to Latent failures, %	Latent multiple-Point failure rate/FIT
HV CONTROL Inputs												
STACK's'_AI_0V1	Connection	1)C24	3.5E-02	Y	3.5E-02	40 %	1.4E-02	Y	50 %	0.0E+00			7.0E-03
FCS_HVPOS_INT_AI_0V1	Connection	1)C25	3.5E-02	Y	3.5E-02	40 %	1.4E-02	Y	50 %	7.0E-03	PCc_HV_C_COMP	60 %	2.8E-03
FCS_HVPOS_EXT_AI_0V1	Connection	1)C26	3.5E-02	Y	3.5E-02	40 %	1.4E-02	Y	50 %	7.0E-03	PCc_HV_C_COMP	60 %	2.8E-03
STACK's'_AI_0A001	Transducer	1)T7	4.0E+01	Y	4.0E+01	40 %	1.6E+01	Y	50 %	7.0E-03			7.8E+00
FCS_AI_0A001	Transducer	1)T8	4.0E+01	Y	4.0E+01	40 %	1.6E+01	Y	50 %	7.8E+00			7.8E+00
HV CONTROL Internals												
HVNEG_DHO_V	Actuator	1)A1	3.0E+01	Y	3.0E+01	40 %	8.6E+00	Y	50 %	0.0E+00			4.3E+00
HVPOS_PRECHG_HDO_V	Actuator	1)A10	1.2E+01	Y	1.2E+01	40 %	4.7E+00	Y	50 %	4.3E+00			2.4E+00
HVPOS_HDO_V	Actuator	1)A2	1.9E+02	Y	1.9E+02	40 %	5.5E+01	Y	50 %	2.4E+00			2.7E+01
HV CONTROL Outputs												
HVNEG_AO_V	Connection	1)C4	3.0E+00	Y	3.0E+00	40 %	0.0E+00	Y	50 %	0.0E+00			0.0E+00
HVPOS_AO_V	Connection	1)C5	3.0E+00	Y	3.0E+00	40 %	0.0E+00	Y	50 %	0.0E+00			0.0E+00
STACK CONTROL Inputs												
STACK's'_AI_0V1	Measurement	1)M2	4.0E+00	Y	4.0E+00	40 %	1.6E+00	Y	50 %	0.0E+00			7.8E-01
FCS_HVPOS_INT_AI_0V1	Measurement	1)M3	6.0E+00	Y	6.0E+00	40 %	2.4E+00	Y	50 %	7.8E-01	PCc_HV_C_COMP	60 %	4.7E-01
FCS_HVPOS_EXT_AI_0V1	Measurement	1)M4	6.0E+00	Y	6.0E+00	40 %	2.4E+00	Y	50 %	1.2E+00	PCc_HV_C_COMP	60 %	4.7E-01
STACK's'_AI_0A001	Measurement	1)M18	6.0E+00	Y	6.0E+00	40 %	2.4E+00	Y	50 %	1.2E+00			1.2E+00
FCS_AI_0A001	Measurement	1)M19	4.0E+00	Y	4.0E+00	40 %	1.6E+00	Y	50 %	1.2E+00			7.8E-01
CELL'c'_AI_0V0001	Data	1)D3	8.3E-01	Y	8.3E-01	40 %	3.0E-01			7.8E-01			
STACK's'_AI_0V001	Data	1)D4	8.3E-01	DS	0.0E+00	40 %	3.3E-01			0.0E+00			

STACK's'_AI_0C1	Data	1) D29	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	0.0E+00			1.5E-01
FCS_AIR_IN_POS_AI_1Dg	Data	1) D39	8.3E-01	DS	0.0E+00	40 %	3.3E-01			1.5E-01			
STACK's'_EXHAUST_POS_AI_1Dg	Data	1) D40	8.3E-01	DS	0.0E+00	40 %	3.3E-01			0.0E+00			
STACK's'_FAN'f'_FI_HZ	Measurement	1) M6	4.0E+00	DS	0.0E+00	40 %	1.6E+00			0.0E+00			
STACK's'_TEMP't'_AI_0C1	Measurement	1) M7	4.0E+00	Y	4.0E+00	40 %	0.0E+00			0.0E+00			
CATHODE_AIR_AI_0Pa1	Measurement	1) M17	4.0E+00	DS	0.0E+00	40 %	1.6E+00			0.0E+00			
H2_VALVE_AfbI_0V1	Measurement	1) M8	4.0E+00	DS	0.0E+00	40 %	1.6E+00			0.0E+00			
H2_VALVE_AfbI_0A001	Measurement	1) M9	4.0E+00	DS	0.0E+00	40 %	1.6E+00			0.0E+00			
H2_PRESS_AI_0Pa1	Measurement	1) M15	4.0E+00	DS	0.0E+00	40 %	1.6E+00			0.0E+00			
STACK's'_PURGE_VALVE_AfbI_0V1	Measurement	1) M13	4.0E+00	DS	0.0E+00	40 %	1.6E+00			0.0E+00			
STACK's'_PURGE_VALVE_AfbI_0A001	Measurement	1) M14	4.0E+00	DS	0.0E+00	40 %	1.6E+00			0.0E+00			
STACK's'_PURGE_POS's'_DHI_V	Measurement	1) M12	4.0E+00	DS	0.0E+00	40 %	1.6E+00			0.0E+00			
DILUTION_FAN_FI_1HZ	Measurement	1) M16	4.0E+00	DS	0.0E+00	40 %	1.6E+00			0.0E+00			
H2_AI_0PC1	Data	1) D10	8.3E-01	DS	0.0E+00	40 %	3.3E-01			0.0E+00			
FCS_CMD_DP_RX	Data	1) D5	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	0.0E+00	PCc_WDOG	90 %	1.5E-02
STACK's'_FAN'f'_AfbI_0V1	Measurement	1) M21	4.0E+00	DS	0.0E+00	40 %	1.6E+00			1.5E-01			
STACK's'_FAN'f'_AfbI_0A1	Measurement	1) M22	4.0E+00	DS	0.0E+00	40 %	1.6E+00			0.0E+00			

STACK CONTROL Internals

SAFE_DP	Parameter	1)P56	1.6E-01	DS	0.0E+00	40 %	6.6E-02			0.0E+00			
FCS_STATE_DP	Parameter	1)P7	1.6E-01	Y	1.6E-01	40 %	6.4E-02	Y	50 %	0.0E+00	PCc_WDOG	90 %	3.2E-03
CAL_WINDOW_DP_0V001	Parameter	1)P57	2.1E-02	Y	2.1E-02	40 %	8.1E-03			3.2E-02			

STACK CONTROL Outputs

HVNEG_DHO_V	Output	1) O1	1.2E+01	Y	1.2E+01	40 %	4.7E+00	Y	50 %	0.0E+00			2.4E+00
HVPOS_DHO_V	Output	1) O2	1.2E+01	Y	1.2E+01	40 %	4.7E+00	Y	50 %	2.4E+00			2.4E+00
HVPOS_PRECHG_DHO_V	Output	1) O1	1.2E+01	Y	1.2E+01	40 %	4.7E+00	Y	50 %	2.4E+00			2.4E+00

		7											
FCS_AIR_IN_PO_0PC1	Data	1) D37	8.3E-01	Y	8.3E-01	40 %	3.2E-01	Y	50 %	2.4E+00			1.6E-01
STACK's'_EXHAUST_PO_0PC1	Data	1) D38	8.3E-01	Y	8.3E-01	40 %	3.2E-01	Y	50 %	1.6E-01			1.6E-01
STACK's'_FAN'f'_DHO_V	Output	1) O6	1.2E+01	Y	1.2E+01	40 %	4.7E+00			1.6E-01			
STACK's'_FAN'f_PO_0PC1	Output	1) O7	1.2E+01	Y	1.2E+01	40 %	4.7E+00			0.0E+00			
H2_VALVE_PO_0PC1	Output	1) O10	1.2E+01	Y	1.2E+01	40 %	4.7E+00			0.0E+00			
H2_VALVE_SO_0V	Output	1) O11	1.2E+01	Y	1.2E+01	40 %	0.0E+00			0.0E+00			
STACK's'_PURGE_VALVE_DHO_V	Output	1) O12	1.2E+01	Y	1.2E+01	40 %	4.7E+00			0.0E+00			
PURGE_VALVES_SO_0V	Output	1) O13	1.2E+01	Y	1.2E+01	40 %	0.0E+00			0.0E+00			
STACK's'_PURGE_HEAT's'_DHO_V	Output	1) O14	1.2E+01	N	0.0E+00	40 %	4.8E+00			0.0E+00			
PURGE_HEAT_SO_0V	Output	1) O15	1.2E+01	N	0.0E+00	40 %	4.8E+00			0.0E+00			
DILUTION_FAN_SO_0V	Output	1) O19	1.2E+01	Y	1.2E+01	40 %	0.0E+00	Y	50 %	0.0E+00			0.0E+00
DILUTION_FAN_PO_0PC1	Output	1) O16	1.2E+01	Y	1.2E+01	40 %	4.7E+00	Y	50 %	0.0E+00			2.4E+00
FCS_0A001_DP_TX	Data	1) D19	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	2.4E+00	PCc_WDOG	90 %	1.5E-02
FCS_0V01_DP_TX	Data	1) D20	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	1.5E-01	PCc_WDOG	90 %	1.5E-02
FCS_1W0_DP_TX	Data	1) D21	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	1.5E-01	PCc_WDOG	90 %	1.5E-02
FCS_MAX_DCH_0A01_DP_TX	Data	1) D22	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	1.5E-01	PCc_WDOG	90 %	1.5E-02
FCS_MIN_DCH_0V001_DP_TX	Data	1) D23	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	1.5E-01	PCc_WDOG	90 %	1.5E-02
STACK's'_AI_0A001_DP_TX	Data	1) D24	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	1.5E-01	PCc_WDOG	90 %	1.5E-02
STACK's'_AI_0V01_DP_TX	Data	1) D25	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	1.5E-01	PCc_WDOG	90 %	1.5E-02
STACK's'_1W0_DP_TX	Data	1) D26	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	1.5E-01	PCc_WDOG	90 %	1.5E-02
FCS_STATUS_DP_TX	Data	1) D6	8.3E-01	Y	8.3E-01	40 %	3.0E-01	Y	50 %	1.5E-01	PCc_WDOG	90 %	1.5E-02
CELL CONTROL													
Inputs													
CELL'c'_AI_0V0001	Measurement	1) M1	4.0E+00	Y	4.0E+00	40 %	5.6E-01			0.0E+00			

STACK's'_AI_0V0001	Measurement	1)M23	4.0E+00	DS	0.0E+00	40%	1.6E+00			0.0E+00			
CELL'c'_AI_0C1	Measurement	1)M20	4.0E+00	DS	0.0E+00	40%	1.6E+00			0.0E+00			
CELL'c'_CVL_HSDO	Data	1)D32	8.3E-01	Y	8.3E-01	40%	3.0E-01	Y	50%	0.0E+00	PCc_OA_WINDOW	60%	6.0E-02
CELL CONTROL Outputs													
CELL'c'_AI_0V0001	Data	1)D1	8.3E-01	Y	8.3E-01	40%	3.0E-01			0.0E+00			
STACK's'_AI_0V001	Data	1)D2	8.3E-01	DS	0.0E+00	40%	3.3E-01			0.0E+00			
STACK's'_AI_0C1	Data	1)D30	8.3E-01	DS	0.0E+00	40%	3.3E-01			0.0E+00			
Cell Inputs													
CELL'c'_AI_0V0001	Connection	1)C1	3.5E-02	Y	3.5E-02	40%	6.8E-03			0.0E+00			
CELL'c'_AI_0V0001	Connection	1)C2	3.5E-02	DS	0.0E+00	40%	1.4E-02			0.0E+00			
CELL'c'_AI_0C1	Connection	1)C3	3.5E-02	DS	0.0E+00	40%	1.4E-02			0.0E+00			
Inlet Air Control Inputs													
FCS_AIR_IN_PI_0PC1	Data	1)D33	8.3E-01	Y	8.3E-01	40%	3.0E-01	Y	50%	0.0E+00			1.5E-01
FCS_AIR_IN_POS_AI_1Dg	Transducer	1)T10	4.0E+01	DS	0.0E+00	40%	1.6E+01			1.5E-01			
Inlet Air Control Outputs													
FCS_AIR_IN_PO_0PC1	Actuator	1)A12	8.0E+01	Y	8.0E+01	40%	2.3E+01	Y	50%	0.0E+00			1.1E+01
FCS_AIR_IN_POS_AI_1Dg	Data	1)D34	8.3E-01	DS	0.0E+00	40%	3.3E-01			1.1E+01			
Exhaust Control Inputs													
STACK's'_EXHAUST_PI_0PC1	Data	1)D35	8.3E-01	Y	8.3E-01	40%	3.0E-01	Y	50%	0.0E+00			1.5E-01
STACK's'_EXHAUST_POS	Transducer	1)T11	4.0E+01	DS	0.0E+00	40%	1.6E+01			1.5E-01			
Exhaust Control Outputs													
STACK's'_EXHAUST_PO_0PC1	Actuator	1)A13	8.0E+01	Y	8.0E+01	40%	2.3E+01	Y	50%	0.0E+00			1.1E+01
STACK's'_EXHAUST_POS	Data	1)D36	8.3E-01	DS	0.0E+00	40%	3.3E-01			1.1E+01			
Stack Fans Inputs													
STACK's'_FAN'f'_HSDO	Connection	1)C6	3.5E-02	Y	3.5E-02	40%	1.4E-02			0.0E+00			
STACK's'_FAN'f'_PWM	Connection	1)C7	3.5E-02	Y	3.5E-02	40%	1.4E-02			0.0E+00			
STACK's'_FAN'f'_HZ	Transducer	1)T1	4.0E+01	DS	0.0E+00	40%	1.6E+01	Y	50%	0.0E+00			8.0E+00
STACK's'_TEMP't'_AI_0C1	Transducer	1)T2	2.0E+00	Y	2.0E+00	40%	0.0E+00			8.0E+00			
Stack Fans Outputs													
STACK's'_FAN'f'_HSDO	Actuator	1)A3	1.5E+01	Y	1.5E+01	40%	3.6E+00			0.0E+00			

STACK's'_FAN'f'_PWM	Actuator	1)A4	1.0E+02	Y	1.0E+02	40%	4.0E+01			0.0E+00			
STACK's'_FAN'f'_HZ	Connection	1)C8	3.5E-02	DS	0.0E+00	40%	1.4E-02	Y	50%	0.0E+00			7.1E-03
STACK's'_TEMP't'_AI_0C1	Connection	1)C9	2.0E+00	Y	2.0E+00	40%	6.5E-01			7.1E-03			
Cathode Air Pressure Inputs													
CATHODE_AIR_AI_0PA1	Transducer	1)T6	4.0E+01	DS	0.0E+00	40%	1.6E+01			0.0E+00			
Cathode Air Pressure Outputs													
CATHODE_AIR_AI_0PA1	Connection	1)C23	3.5E-02	DS	0.0E+00	40%	1.4E-02			0.0E+00			
H2 Valve Inputs													
H2_VALVE_PWM	Connection	1)C12	3.5E-02	Y	3.5E-02	40%	5.9E-03			0.0E+00			
H2_VALVE_SO_0V	Connection	1)C13	3.5E-02	Y	3.5E-02	40%	4.7E-03			0.0E+00			
H2 Valve Outputs													
H2_VALVE_PWM	Actuator	1)A7	5.0E+01	Y	5.0E+01	40%	2.0E+01	Y	50%	0.0E+00			9.9E+00
H2 Pressure Inputs													
H2_PRESS_AI_PA	Transducer	1)T3	4.0E+01	DS	0.0E+00	40%	1.6E+01	Y	50%	0.0E+00			8.0E+00
H2 Pressure Outputs													
H2_PRESS_AI_PA	Connection	1)C19	3.5E-02	DS	0.0E+00	40%	1.4E-02	Y	50%	0.0E+00			7.1E-03
Purge Valve Inputs													
STACK's'_PURGE_VALVE_HSDO	Connection	1)C14	3.5E-02	Y	3.5E-02	40%	6.8E-03			0.0E+00			
PURGE_VALVES_SO_0V	Connection	1)C15	3.5E-02	Y	3.5E-02	40%	5.9E-03			0.0E+00			
STACK's'_PURGE_POS's'_DHI_V	Transducer	1)T14	4.0E+01	DS	0.0E+00	40%	1.6E+01	Y	50%	0.0E+00			8.0E+00
STACK's'_PURGE_HEAT's'_DHO_V	Connection	1)C16	3.5E-02	N	0.0E+00	40%	1.4E-02			8.0E+00			
PURGE_HEAT_SO_0V	Connection	1)C17	3.5E-02	N	0.0E+00	40%	1.4E-02			0.0E+00			
Purge Valve Outputs													
STACK's'_PURGE_VALVE_DHO_V	Actuator	1)A8	5.0E+01	Y	5.0E+01	40%	1.4E+01			0.0E+00			
STACK's'_PURGE_POS's'_DHI_V	Connection	1)C18	3.5E-02	DS	0.0E+00	40%	1.4E-02	Y	50%	0.0E+00			7.1E-03
STACK's'_PURGE_HEAT's'_DHO_V	Actuator	1)A14	5.0E+01	N	0.0E+00	40%	2.0E+01			7.1E-03			
Dilution Fan Inputs													
DILUTION_FAN_PO_0PC1	Connection	1)C20	3.5E-02	Y	3.5E-02	40%	6.8E-03			0.0E+00			
DILUTION_FAN_SO_0V	Connection	1)C30	3.5E-02	Y	3.5E-02	40%	6.8E-03			0.0E+00			
DILUTION_FAN_FI_1HZ	Transducer	1)T4	4.0E+01	DS	0.0E+00	40%	1.6E+01	Y	50%	0.0E+00			8.0E+00
Dilution Fan Outputs													
DILUTION_FAN_FI_HZ	Connection	1)C21	3.5E-02	DS	0.0E+00	40%	1.4E-02			0.0E+00			
DILUTION_FAN_PO_0PC1	Actuator	1)A9	1.0E+02	Y	1.0E+02	40%	2.9E+01			0.0E+00			
H2 Sensor Inputs													
H2_AI_oPC!	Transducer	1)T5	1.0E-02	Y	1.0E-02	40%	0.0E+00	Y	50%	0.0E+00			0.0E+00

H2 Sensor Outputs													
H2_AI_oPC1	Connection	1)C22	3.5E-02	Y	3.5E-02	40 %	1.4E-02	Y	50 %	0.0E+00			7.0E-03
Isolation tester													
Isot (previous calc)	Isot	-	9.2E+01	Y	9.2E+01	40 %	3.6E+01	Y	50 %	0.0E+00		90 %	1.8E+00
High Voltage Interlock													
HVIL (estimate)	HVIL	-	4.0E+01	Y	4.0E+01	40 %	1.6E+01	Y	50 %	0.0E+00		90 %	7.9E-01
			1526.8		1113.7								131.120
										Latent Fault metric			87.2%

4.4.5.2 Results Evaluation

The final values are SPFM = 94.2% and LFM = 87.2% which would mean that the architectural metrics can achieve ASIL B for a safety goal 'maintain power within the required operating region'. As discussed in many the PCc claims for diagnostic coverage, many items have conservative claims due to lack of information on the transducers and actuators for this proof of concept design. However, there is good coverage of most elements and the analysis has uncovered the weaker areas which require further investigation.

4.4.5.3 Investigation Areas.

Many points require further investigation:

1) Mechanical linkages reduce the claim as the feedback mechanism does not cover them sufficiently. This can be tackled in one of two ways:
    a. Mechanically move the feedback position so that it represents the damper positions rather than the mechanical link that drives the dampers.
    b. By adding further characteristic analysis so that a PCc can be developed for the control loop and demand positions against damper feedback. This would allow position to be monitored as a diagnostic element only. Characterisation will have to ensure that inlet and outlet failures can be correctly diagnosed.
2) Hydrogen gas monitoring in the exhaust. At the moment there is the possibility that this is included in control loops for purge. If this can be removed, possibly by improved purge valve position monitoring then the hydrogen sensor can be purely for diagnostic purposes. It is likely that this can be removed from this safety goal in terms of consideration for maintaining the correct power. However, consideration will have to be given to other safety goals in terms of safe ventilation of hydrogen which may still require this sensor unless chemical analysis and air flow analysis can prove it was not a safety concern.

3) External measures can be increased by placing requirements on:
    a. The DCDC converter to provide independent measurement of voltage and current. If this is possible at an appropriate ASIL then it may be possible to remove some of the sensing in the FCCS in terms of voltage and current. This would depend on each application and only be recommended for complete removal if the DCDC converter system became a standard part used in every application.
    b. The hybrid controller for verification of signals from the FCCS via measurements after the DCDC converter in terms of power delivery. Again, this can be recommended as standard if a common hybrid controller was to be used. If the controller varied in each application, a more overall cost-efficient solution may be to maintain the proposed level of diagnostic coverage in the FCCS itself to reduce the burden of an additional functional safety impact analysis for every new application.

4.4.5.4 Next Steps.

This is a very early stage on the concept for a FCCS meeting BS ISO 26262 but the methods give a very good indication that the base control system already has relatively good architectural metrics even when conservative estimates are used. The next steps would be:

1) Complete a full HARA to identify all the safety goals.
2) Use this method for each safety goal in turn and identify the architectural metrics that can be claimed against each of the safety goals.
3) Compare results for each safety goal to identify methods to improve diagnostics that either increase independence or provide coverage for faults that have lower coverage percentages at present.
4) Develop different candidate architectures following a similar approach to that applied for the Isolation Tester in 4.2 and the Battery Management System in 4.3.

4.4.5.5 PCc Method Benefits for FCCS analysis.

The analysis has provided a very good insight into the FCCS from an architectural metrics viewpoint. All the work completed so far can now be taken forwards to analyse other safety goals and additional candidate architectures applicable to the FCCS.

To develop a production intent solution, the final architectural metrics and failure rates for the actual hardware design would be obtained and used to improve the failure rates assumed for the lumped element blocks to mature the model. Increasing maturity levels was discussed in 3.7.3.1. This will further improve PCc analysis for future FCCS designs as technology improves and new concepts require evaluation.

4.5 Summary

The method has been applied to three practical applications (4.2 to 4.4). In the first two cases, the Isolation Tester (4.2) and the Battery Management System (4.3) a full analysis has been performed to allow comparison between the predicted results using the PCc method and those achieved with the full analysis.

In both cases, the method has allowed a safety goal to be selected and several candidate architecture proposals to be analysed. Based on the quantified analysis of each proposed architecture, design changes have been developed and the method applied iteratively. From these results, a candidate architecture has been selected to take forward into the full system design lifecycle.

Confidence in the PCc prediction is demonstrated in the results comparison to the values calculated for the final design as shown in Figure 17 and Figure 18 for the Isolation tester and Figure 30 and Figure 31 for the Battery Management System.

Considering the errors for the Isolation Tester (plotted in Figure 38) the errors are always positive showing the pessimistic claim for both SPFM and LFM predictions. As the SPFM and LFM claims improve i.e. tend towards those required for ASIL B, C and D then the errors reduce to a maximum of 1.72 % for the SPFM and 2.01% for the LFM which is considered acceptable when choosing the architecture to take forwards. As the diagnostic claims rely both on a software algorithm and hardware capable of delivering the necessary data for the software algorithm input (and in some cases outputs where test patterns are used) the main criteria is to ensure that the hardware is capable of achieving the architectural metrics for the required ASIL attribute for the safety goal under consideration.

Architectures 1 and 2 have relatively low SPFM and LFM values as the architectures have limited diagnostic coverage against different failures. Architecture 3 provides a significant jump (approx. 11.6% in SPFM see 4.2.5.15). As the diagnostic coverage increases so does the SPFM and LFM and this also links to the reduction in error between the PCc prediction and the final design values.

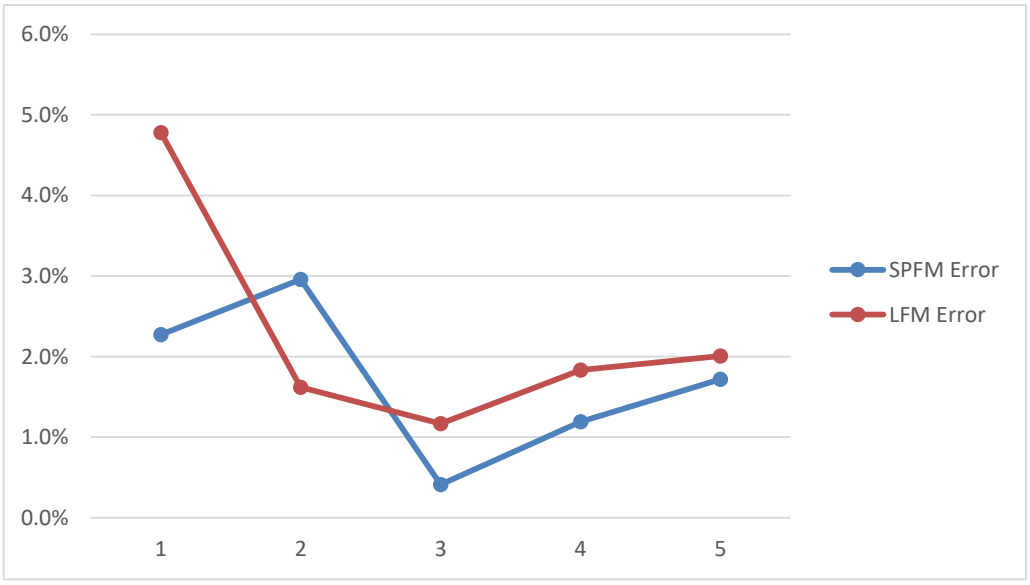


Figure 38: Measure Isolation Resistance SPFM and LFM Errors for Candidate Architectures

The Battery management System errors are shown in Figure 39.

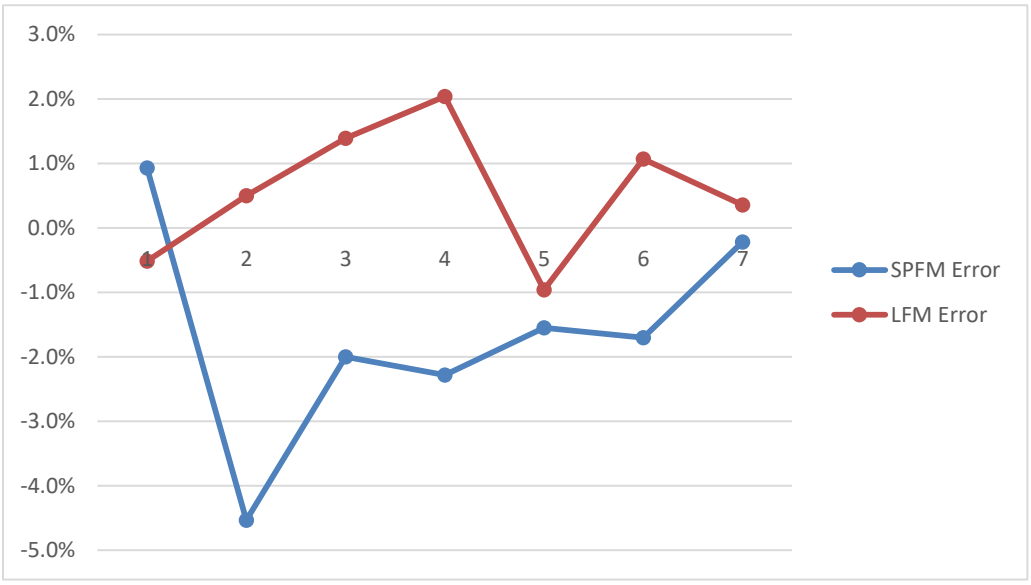


Figure 39: Battery Management System SPFM and LFM Errors for Candidate Architectures

In Isolation Measurement case (Figure 38) the SPFM and LFM values are optimistic i.e. that achieved in the final design was slightly higher than that predicted. In the Battery Management System, the SPFM and LFM values vary around positive and negative. Other than architecture 2 which utilised the limited hardware architecture the errors are still within +/- 2.3% and as the architecture improves the errors reduce. In architecture 2 there is also a large bias towards the string hardware logic outputs and contactors which contribute a high proportion of the undiagnosed failure rate (20%) compared to the other safety related components in the system when analysed using the PCc method. In the final architecture there is a much higher level of componentry which means that

these components only contribute to 15% of the undiagnosed total failure rate. This may be due to an over simplification in the hardware only route when considered in the PCc route compared to the final design. Further analysis and the implications of the error values are provided in the conclusions (5.2).

In the third example (4.4) the approach shows that the method can be applied very early in the concept stage when exploring possibilities for a new system i.e. if a company wished to embark on developing a fuel cell control system what level of architectural metrics can be achieved based on an initial design feasibility study. This application is very useful and will be used in the future when looking at new technology projects. An example would be autonomous vehicles, where innovative technology is being introduced at a high rate. In this example it would be relatively simple to determine PCcs required to mitigate the main failure modes identified through an FMEA on a preliminary design even though the detail of how this might be achieved in the final hardware is still to be determined.

It may be that some PCcs defined at the concept level may not even be technically possible due to limitations in the hardware or software. This may lead to further research work being undertaken.

The advantage of applying this method is that the requirement for additional research / development work is identified at the concept stage and not delayed until late into the hardware / software design when it becomes apparent that the architectural metrics cannot be achieved due to a limitation in applying the selected diagnostic techniques.

5 Conclusions

The hypothesis made at the beginning of the research was:

> ***'Complex system architectures can be analysed and compared by quantitative methods based on architectural metric calculations at the signal level during the concept stage of product development to accurately predict the single point and latent point fault metrics calculated for the final design'***

The method developed during the work has shown that architectures can be quantified at the concept stage, multiple candidates designed and compared in a quantified way and a design concept selected based on the best architecture with the required level of architectural metrics.

The method is easily understood and very efficient in analysing different concepts.

The actual correlation between PCc predicted architectural metrics and those achieved in the design were sufficiently accurate to give confidence that the process determined the correct Automotive Safety Integrity Level for the architectural metrics parameter required for the design.

The above is discussed in more detail below.

5.1 Method Review and Benefits

The PCc quantification method developed has been shown to provide:

1) A systematic approach to define the function of interest – the system description (3.5). The final element classification is limited to seven classifications (3.5.2) Connections, Measurements, Transducers, Data, Parameters, Outputs and Actuators. This is sufficient to describe any control system accurately in any domain; it is not just restricted to automotive.
2) Easily understood system diagrams (for example Figure 11 and Figure 12) specifically targeted at the analysis of architectural metrics are developed based on the element classifications. The system diagrams identify all the critical elements and lend themselves to analysis of the possible failures in each element. The diagrams clearly show independence within the system and the interfaces between arrays of systems (Figure 19). This facilitates discussions between different internal departments / engineering disciplines and external suppliers etc.
3) Each system diagram can be annotated to show elements that can violate the safety goal being analysed. This clearly identifies which areas require diagnostic coverage and allows PCcs (3.6.3) to be developed that specifically diagnose the faults of interest. The clarity of

independence between systems simplifies discussions relating to ASIL decomposition of requirements.

4) A technique to quantify several candidate architectures to predict Single Point Fault (3.7.1.1) and Latent Fault (3.7.1.4) architectural metrics. This is achieved through two spreadsheet work books, one for the SPFM / LFM calculations (although broken out into two tables for presentation purposes in the Thesis) and a workbook that contains a macro-enabled worksheet for each of the seven element classifications and the power supply function. The element worksheets allow failure modes to be deselected if not required in the design (i.e. failure modes that will not violate the safety goal) and failure mode percentages to be reallocated based on the failure modes of interest. One or more PCcs is then used to provide diagnostic coverage (3.6.2).
5) PCc claims based on known methods for diagnosing failures as defined in functional safety standards. Combining these methods gives a higher confidence that the final design will achieve the required architectural metric requirements. This method is generic and can be tailored to many different safety standards where architectural metrics are required to evaluate the capability of the system to detect failure modes. For example, it can be used for single point fault metrics in line with BS ISO 262622 (BSI, 2011e) or safe fail fractions as in BS EN 61508 part 2 (BSI, 2010).
6) Accurate predictions of SPFM and LFM architectural metrics. This has been demonstrated through the comparison to results from final design solutions.
7) PCc method that is quick to apply, with efficiency improving each time it is applied. Being efficient, it permits many different candidate architectures to be explored and a quantified comparison made between each one. For example, the Isolation Measurement Architecture 5 (4.2.5.25) analysis required 16 elements to be considered in the calculations whereas the final design required analysis of 149 components. For the battery Management System Architecture 7 (4.3.6.35) 45 elements were analysed in the PCc analysis against 895 components in the final design. This is a significant saving in effort especially in the concept stage when a fast technique is required to analyse a candidate architecture.
8) A method that can be matured through continuous improvement as Companies complete additional designs.
9) Influence on decisions as to whether to implement safety features in hardware or software. For a high-volume product it may be better to develop the functionality in software (requiring significant development time) rather than in hardware which increases component cost. If amortisation of software costs over the volume is cheaper than the

increase in hardware cost then this may be beneficial. The PCc method allows this decision to be made early in the design process.

10) Early component selection. Where components offer different diagnostic techniques but a similar functional performance, using PCc techniques early in the process may lead to selection of a particular device – for example, the AFE in the BMS.
11) A method that can be applied to IEC 61508 and ISO26262 as discussed in 3.7.1.3.
12) Right first-time design. This will always be a matter for debate as the design process and final product always has compromises. The PCc method aids the concept analysis and significantly leads to an improved architecture. In all examples completed so far, the architecture developed and selected via the PCc Method has always:
    a. Delivered the required architectural metrics in the final design.
    b. Led to an architecture with well-defined independence that supports ASIL decomposition.
    c. Removed any iterative loops relating to system architecture design in the system design stage.
    d. Front loaded the project definition heavily to the concept stage.
    e. Given clear traceable diagnostic requirements based on the PCcs.
    f. Elicits requirements early in the design process.

5.2 Accuracy of Quantification Results

As shown in the results sections for the Isolation Tester (4.2.6) and the Battery Management System (4.3.7), very close correlation is achieved between the predicted SPF and LF architectural metrics using the PCc Quantification Method and the final analysis completed as per BS ISO26262 part 5 (BSI, 2011e).

Although the diagnostic coverage, SPFM and LFM percentages are quantified values their determination relies heavily on base data. Where possible, definitive data is used, each failure mode is individually assessed, this failure mode is apportioned a percentage of the overall failure rate and the diagnostic coverage defined. However, all of this is related to the accuracy of the base data. Often, with component suppliers, the data is relatively generic for a type of device. For example, an intelligent output driver may be based on a technology platform rather than the specific individual part and failure modes may be generalised. This data is sometimes predicted rather than being justified by field data. If field data is used, engineering judgement is required to ensure confidence that that the failure mode and occurrence is diagnosed and reported accurately.

If the variance relates to specific components then the architectural metrics for those components provided by the manufactures (especially for complex components) should be compared to the assumptions made when performing the PCC calculations. Variance can occur where the supplier has made different assumptions in terms of safe failures, fault detection measures etc. when performing their own internal analysis. Often manufactures must design the 'element out of context' in order to provide a generic component for use in many applications and it may be possible to obtain more accurate results by discussing the specific application.

The outcome is that there is always a small error in the actual architectural metric results and this can only be improved over time as data is gathered by component suppliers, Tier 1 suppliers and OEMs and this information is openly shared.

One important aspect of continuous improvement is the way in which complex semiconductors are being handled. In the first edition of BS ISO 26262 (BSI, 2011e), where no additional information is available, failure modes may be considered 50% safe and 50% leading to violation of the safety goal. However, in edition 2 there is a new draft ISO / DIS 26262 part 11 (ISO/DIS 26262-11, 2016) which offers significantly more information on failure modes relating to complex semiconductors.

The above leads to the conclusion that the relative comparison between the architectures are accurate due to repetitive use of base data in each candidate architecture but that there is always a level of uncertainty in the absolute SPFM and LFM percentages. This is applicable both to the PCc predictions and the end results for the detailed design.

5.3 Lessons Learnt

One of the aims of the method is to significantly reduce time in the analysis process so that it can be conducted on multiple candidates at the concept stage. This was achieved, however, the amount of effort required to develop the full designs and associated architectural metrics for each candidate was severely underestimated. This added a considerable amount of time to the proof but could not be avoided as the predictions had to be verified to give merit to the developed method. This delayed completion of the PhD but also supports the claim that the PCc method is very efficient and ideally suited to concept evaluation.

Without the PCc Method, a designer could complete the design, perform the detailed architectural metrics calculation and then identify a major floor in the architecture. This would significantly delay the project, add costs and increase time to market.

The naming convention was a late addition to the proposed method and really came about due to the difficulty in tracing signals through the design and into the final electronic circuit. This meant many iterations as the method developed, with changes to names so that they made sense schematically and could be traced reliably through the design in a logical manner. There was also confusion, in some cases, between the resolution of signals and whether the PCc claim was justified when comparing signals if the resolution was not defined. This convention was added into the process during the development of the BMS and retrospectively applied to the Isolation tester. This is now an important part of the PCc method and plays a valuable role in traceability from concept through to final design.

Some confusion arose around defining elements and signals that could violate the safety goal and those used purely for diagnostics. To eliminate this confusion, the FCCS description contains a specific colour (yellow in this case) to highlight elements and signals that need to be considered as they form part of the diagnostics. Typically, they would not in themselves lead directly to the violation of the safety goal if they failed but they will contribute to an improvement in the fault metrics and may also impact on maintaining the system in a safe state.

On a personal note, the work has greatly improved my research skills:

- When conducting reviews all material is annotated electronically and indexed or relevant information recorded in a central data resource that can easily be indexed. This not only proved useful in the Thesis but also on other work-related projects where material has been reference or additional reviews performed.
- Peer reviews are critical to questioning not only what work is being undertaken but why it is being undertaken. This allows priorities to be set and can prevent effort being spent on 'areas of interest' that are maybe not as relevant as first thought.
- Interdisciplinary discussions are vital. Functional safety knowledge within companies is often quite restricted and treated almost as a standalone function for design analysis and monitoring. Pulling the functional safety experts into the technology concepts very early on in the process really promotes discussion and a thorough investigation of all possible design solutions.

5.4 Additional Benefits

A number of interesting benefits were detected that were not originally identified as required outcomes. These are discussed below.

5.4.1 Comparison between Design Approaches

The Battery Management System demonstrated that two completely distinctive design approaches could be compared. Architecture 1 used a predominantly software based approach and architecture 2 relied on a hardware approach. Both were valid design solutions but the hardware approach was more suited to a proof of concept where many different control techniques / software algorithms were to be developed with the safety being provided by the hardware shutdown system. The software approach relied considerably more on having compliant software processes and emphasis being placed on software testing to prove all safety requirements were satisfied and verified prior to putting into service.

If the intention was to provide a proof of concept solution then Architecture 2 could have been developed with techniques from architectures 6 and 7 (requiring a certain level of software). The algorithms for voltage measurement and contactor control would be relatively simple to test and verify and would be unlikely to change in different applications. This route may have delivered the required architectural metrics for ASIL C (as required for the safety element out of context system). This could be completed using the PCc method should this design approach be required.

In some cases, as with the FCCS analogue front end, there are limited suppliers that can deliver integrated circuits to fulfil the functional requirements. The PCc method can be used to look at these devices in isolation to understand failure modes and diagnostic coverage based on a lumped model for the required hardware. Assuming more than one supplier was available, the PCc diagnostic claims for each supplier could be used in the SPFM and LFM architectural metric calculations to understand which device delivers the better functional safety performance when used in the application to deliver a specific safety goal.

5.4.2 Diagnostic Requirements Elicitation and Traceability

Because the PCc claims for each of the classified elements is based specifically on the diagnostic techniques covered in BS ISO 26262 part 5 (BSI, 2011e) it becomes a simple task to generate specific hardware and software requirements at the technical safety requirements stage (BSI, 2011d) which are traced back to the concept stage (BSI, 2011c). It is important because it means that a lot of the technical design is inherent at the concept stage (via the PCc diagnostic coverage claim) but does not need detailed implementation requirements until later in the process. It also means that the diagnostic requirements are well understood and once the system design is started the diagnostic functions can be allocated to hardware or software, or, as is more common, a combination of the two.

5.4.3 Evaluation of Required Diagnostic Coverage Claims

As discussed in the Progressive Approach (3.8.1), it is possible to update the SPFM and LFM spreadsheets with trial values for diagnostic coverage against different elements to see how this will affect the final SPFM and LFM percentages. This cannot be realised easily at the final design stage as a diagnostic technique is likely to involve many components rather than just a single classified element.

This is very useful in understanding which elements to concentrate on when investigating different PCcs and what sort of techniques should be utilised in the PCc to achieve the required level of diagnostic coverage - low, medium or high. Once a target is set, the PCc can be developed with target coverage in mind which will guide the use of specific techniques to cover the failure modes of interest.

5.4.4 Improving Diagnostic Trouble Codes (DTCs)

For lower level ASILs it is not required, or recommended, to perform the SPFM and LFM calculations. This is understandable at the final design stage. However, as the PCc method is quick to apply, completing the PCc analysis for all designs, from QM to ASIL 'D', leads to an elevated level of understanding of the system, failure modes and the faults that can be detected. This can be used to detail requirements for DTCs at the concept stage before running a full requirement check via an FMEA, for example, in the later system design stage. This is of significant benefit to service centres.

5.5 Limitations

The method has been shown to work for control systems that are closely aligned to automotive applications that require a final safety case aligned to ISO26262. This can be a system or array of systems as defined in ISO26262 part 1 (BSI, 2011a). The PCc method is based on the techniques that are required in the final design analysis and application outside of this area has not been analysed although other areas should be considered (see 6).

The failure rate data and failure mode date used in the examples was based on mature data (3.7.3.1) as this data was available. A less accurate data set in the concept stage would reduce accuracy in the SPFM and LFM values however this does not impact on the relative accuracy when comparing candidate architectures as long as the same data is used for each candidate. Refining accuracy as experience matures will increase the accuracy of the results for each candidate.

The method, even with the use of the macro in the spreadsheet is still a manual procedure. Defining the system in terms of an ADL would improve the method and allow for automated calculations of the SPFM an LFM architectural metrics and offer further increases in calculation efficiency, possibly allowing additional candidate architectures to be analysed (see 6).

The method covers the architectural metrics required in standards e.g. ISO26262 (BSI, 2011e) which allows a conceptual candidate to be analysed and then taken through to full design. It does not, nor was it intended to, analyse dependencies between failures and analysis of the probability of random hardware failures which would also be required in the final design analysis when building an overall safety case for the item as this can be achieved by the use of other tools e.g. Hip-HOPS (HiP-HOPS, 2017).

6 Further Work

The proposed method has been used now in many work applications by the author and other engineers and will be used in future safety critical designs to mature the models and develop the functional safety concept.

During the research work many other interesting topics were questioned as discussed below:

1) If a lumped model, which is safety critical, has no coverage will this lead to either a single point fault or a dominant fault when the random hardware failure rates are calculated? This has been considered because the diagnostic coverage effectively puts an 'AND' gate in the fault tree meaning that diagnostic coverage must fail as well as the control element itself. If this is the case then the PCc method can be used to prioritise each lumped model / classified element to ensure an elevated level of diagnostic coverage which will then influence the achievable random hardware failure rates. This would need the fault tree analysis to be performed for each candidate architecture used in the previous examples. For the Battery Management System and the Isolation Tester this would be relatively straightforward as the failure rate data is already available. The real unknown in this approach is the relationship between increased component count (hence increased system failure rate) against the reduction in failure rate for the safety goal of interest due to the improved diagnostic coverage.
2) Tool generation. As the system description is an interconnected block diagram with specific attributes in terms of failure modes, failure mode percentages, diagnostic coverage and an overall diagnostic claim using the PCcs it should be possible to develop an application to calculate the SPFM and LFM for the candidate architecture automatically based on an EAST-ADL (EAST-ADL Association, 2013). This tool could also maintain the data base for all the lumped model data which could then be matured as more architectures are completed. Possible tools that could be considered are Vector PREEvision (Vector PV, 2017), Matlab (Mathworks, 2017) or HipHops (HiP-HOPS, 2017).
3) Other areas of application. As the PCc method looks at failure modes and diagnostic capability could it be applied to other systems? Possible considerations in the automotive setting are exhaust emissions control. Outside of the automotive arena, there are several possible application areas such as banking, supply chain, accounting etc. To be applied suitable metrics would have to be defined or a basic 0-100% scale could be used to identify single points of failure in the system.

7 References

EAST-ADL Association, 2013. *EAST-ADL Domain Model Specification.* [Online]
Available at: https://www.east-adl.info/Specification/V2.1.12/EAST-ADL-Specification_V2.1.12.pdf
[Accessed 16 March 2019].

A123 Systems Inc, 2011. *Nanophosphate® Lithium Ion Prismatic Pouch Cell.* [Online]
Available at: http://liionbms.com/pdf/a123/AMP20M1HD-A.pdf
[Accessed 17 03 2016].

AAAM, 2015. *Abbreviated Injury Scale.* [Online]
Available at: https://www.aaam.org/abbreviated-injury-scale-ais/
[Accessed 18 02 2017].

AMS AG, 2015. *AMS Products HLS-440P Factsheet.* [Online]
Available at: http://ams.com/eng/Products/Environmental-Sensors/Hydrogen-Sensors/HLS-440P-B
[Accessed 05 08 2016].

Andrea, D., 2010. *Battery Management Systems for Large Lithium-Ion Battery Packs.* 1 ed. Norwood: Artech House.

ANSYS medini Technologies AG, 2016. *medini analyze - ISO 26262 integrated in a single tool.* [Online]
Available at: http://www.medini.eu/index.php/de/products/functional-safety
[Accessed 17 03 2016].

Astruc J-M, B. N., 2010. *Toward the application of ISO 26262 for real-life embedded mechatronic systems.* Toulouse, Embedded Real Time Software and Systems.

AUTOSAR, 2016. *Layered Software Architecture,* s.l.: AUTOSAR.org.

Azevedo LdS, P. D. W. M. P. Y., 2014. Assisted Assignment of Automotive Safety Requirements. *IEEE Software,* pp. 62-68.

BOC, 2015. *BOC Safety data Sheet - Hydrogen Compressed.* [Online]
Available at: https://www.boconline.co.uk/internet.lg.lg.gbr/en/images/tg-8360-hydrogen-v1.3410_39605.pdf?v=4.0
[Accessed 05 08 2016].

Brewerton, S., 2011. *Safety Integrity of Vehicle Propulsion Systems.* Troy, Michigan, s.n.

Broadcom, 2014. *BroadR-Reach Physical Layer Transceiver Specification For Automotive Applications.* V3.0 ed. s.l.:Broadcom Corporation.

BSI, 1997. *BS EN 954-1:1997 Safety of Machinery. Safety related parts of control systems. General principles for design..* [Online]
Available at: https://shop.bsigroup.com/ProductDetail/?pid=000000000001048553
[Accessed 08 September 2017].

BSI, 2001. *BS EN 50128:2001 Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems.* [Online]
Available at: https://shop.bsigroup.com/ProductDetail?pid=000000000030228797
[Accessed 08 09 2017].

BSI, 2003. *BS EN 50129:2003 Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling.* [Online]
Available at: https://shop.bsigroup.com/ProductDetail/?pid=000000000030228799
[Accessed 08 09 2017].

BSI, 2004. *PD IEC TR 62380:2004 Reliability data handbook - Universal model for reliability prediction of electronics components, PCBs and equipment.* London: British Standards Institution.

BSI, 2007. *BS EN 61508-0 - Functional safety of electrical/electronic/prorammable electronic safety related systems Part 0: Functional Safety and IEC61508,* London: s.n.

BSI, 2008. *BS 18004 Guide to achieving effective occupational health and safety performance,* s.l.: British Standards Institution.

BSI, 2010a. *BS EN 61508-1 - Functional safety of electrical/electronic/prorammable electronic safety related systems Part 1: General Requirements,* London: British Sandards Institution.

BSI, 2010. *BS EN 61508-2 - Functional safety of electrical/electronic/prorammable electronic safety related systems Part 2: Requirements for electrical/electronic/prorammable electronic safety related systems.* London: British Standards Institution.

BSI, 2010c. *BS EN 61508-4 - Functional safety of electrical/electronic/programmable electronic safety related systems Part 4: Definitions and abbreviations,* London: British Standards Institution.

BSI, 2011a. *BS ISO 26262-1 Road vehicles - Functional safety Part 1: Vocabulary.* London: British Standards Institution.

BSI, 2011b. *BS ISO26262-2 Road vehicles - Functional safety Part 2: Management of functional safety.* London, British Standards Institution.

BSI, 2011. *BS ISO26262-9 Road vehicles - Functional safety Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses.* London: British Standards Institution.

BSI, 2011c. *BS ISO 26262-3 Road vehicles - Functional safety Part 3: Concept phase.* London, British Standards Insitution.

BSI, 2011d. *BS ISO26262-4 Road vehicles - Functional safety Part 4: Product development at the system level.* London, British Standards Institution.

BSI, 2011e. *BS ISO 26262-5 Road vehicles - Functional safety Part 5: Product development at the hardware level.* London, British Standards Institution.

BSI, 2011f. *BS ISO26262-6 Road vehicles - Functional safety Part 6: Product development at the software level.* London, British Standards Institution.

BSI, 2011g. *BS ISO26262-7 Road vehicles - Functional safety Part 7: Production and operation.* London, British Standards Institution.

BSI, 2011h. *BS ISO26262-8 Road vehicles - Functional safety Part 8: Supporting processes.* London, British Standards Institution.

BSI, 2012. *BS EN 62282-2:2012 Fuel cell technologies Part 2: Fuel Cell Modules.* London: British Standards Institute.

BSI, 2012. *BS EN ISO 13849-2 Safety of machinery - Safety-related parts of control systems. Part 2: Validation.* London: British Standards Institution.

BSI, 2012. *BS ISO26262-10 Road vehicles - Functional safety Part 10: Guideline on ISO26262.* London, British Standards Institution.

BSI, 2015. *BS EN ISO 13849-1 Safety of machinery - Safety-related parts of control systems. Part 1: General principles for design.* London: British Standards Institution.

BSI, 2016. *BS EN 60812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA),* London: British Standards Institute.

BSI, 2016. *BS EN 61882 Hazard and operability studies (HAZOP studies) — Application Guide.* London: The British Standards Institution.

BSI, 2016. *Draft BS ISO 26262-1 Road vehicles - Functional safety,* London: British Standards Institute.

CENELEC, 1999. *EN 50126:1999 Railway Applications - The Specification And Demonstration Of Reliability, Availability, Maintainability And Safety (rams).* [Online]
Available at: http://infostore.saiglobal.com/store/details.aspx?ProductID=365276
[Accessed 21 02 2017].

Choo, H. C. D. L. J. S. H. e. a., 2015. *Performance Recovery of Fuel Cell Stack for FCEV.* New York, SAE International, pp. recovery 3,.

Cimatti A, R. M. S. A. T. S., 2010. Formalization and Validation of Safety-Critical Requirements. *Electronic Proceedings in Theoretical Computer Science (EPTCS),* pp. 68-75.

Cuenot P, A. C. A. N. O. S. M. F., 2014. *Applying Model Based Techniques for Early Safety Evaluation of an Automotive Architecture in Compliance with the ISO 26262 Standard.* [Online]
Available at: http://www.bmw-carit.com/downloads/publications/ApplyingModelBasedTechniquesForEarlySafetyEvaluationOfAnAutomotiveArchitecture.pdf
[Accessed 18 04 2016].

DIN VDE, 1990. *DIN V VDE 0801 VDE 0801:1990-01 Principles for computers in safety-related systems.* [Online]
Available at: https://www.vde-verlag.de/standards/0801000/din-v-vde-0801-vde-0801-1990-01.html
[Accessed 21 02 2017].

DIN, 1991. *DIN EN 292-1:1991-11 Safety of machinery; basic concepts, general principles for design; part 1: basic terminology, methodology.* [Online]
Available at: https://www.beuth.de/en/standard/din-en-292-1/1803545
[Accessed 21 02 2017].

DIN, 1994. *DIN V 19250:1994-05 Control technology; fundamental safety aspects to be considered for measurement and control equipment.* [Online]
Available at: http://www.beuth.de/en/pre-standard/din-v-19250/2286682
[Accessed 21 02 2017].

EASA, 2011. *Methodology to Assess Future Risks,* Cologne: European Aviation Safety Agency.

ELVA Consortium, 2013. *Advanced Electric Vehicle Architectures,* Aachen: ELVA.

European Parliment, 2006. *DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC,* s.l.: THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN.

Findeis, M. & Pabst, I., 2006. *Functional Safety in the Automotive Industry, Process and Methods.* Berlin, VDA.

Government of Canada - Transport Canada, 2017. *Defect investigations of motor vehicles, tires, and child car seats.* [Online]
Available at: http://www.tc.gc.ca/eng/motorvehiclesafety/defect-investigations-motor-vehicles.html
[Accessed 18 02 2017].

Habli I, I. I. R. R. K. T., 2010. *Model-Based Assurance for Justifying Automotive Functional Safety,* s.l.: SAE International.

Hauke, M et al, 2008. *Functional safety of machine controls (BGIA Report 2/2008e),* Berlin: Functional safety of machine controls (BGIA Report 2/2008e).

Hecht, M. N. E. C. A. P. J. e. a., 2015. *Creation of Failure Modes and Effects Analyses from SysML,* Warrendale: SAE Intenational.

Hillenbrand M, H. M. M.-G. K. A. N. M. J. R. C., 2010. *An Approach for Rapidly Adapting the Demands of ISO/DIS 26262 to Electric/Electronic Architecture Modelling.* Fairfax, Virginia, USA, IEEE.

HiP-HOPS, 2017. *Hierarchically Performed Hazard Origin and Propagation Studies.* [Online]
Available at: http://hip-hops.eu/
[Accessed 08 08 2017].

HSE, 2001. *Reducing risks, protecting people.* Norwich: Her Majesty's Stationary Office.

HSE, 2004. *A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented be dafety-related electrical, electronic and programmable electronic systems of machines,* Norwich: Her Majesty's Stationary Office.

IBM, 2017. *IBM Rational Rhapsody Architect for Systems Engineers.* [Online]
Available at: https://www.ibm.com/us-en/marketplace/architect-for-systems-engineers
[Accessed 08 03 2017].

IEC, 1965. *IEC 60204-1 Safety of machinery - Electrical equipment of machines - Part 1: General requirements.* [Online]

Available at: https://webstore.iec.ch/publication/26037
[Accessed 21 02 2017].

IEC, 1998. *IEC 61508-1:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements.* [Online]
Available at: https://webstore.iec.ch/publication/19800
[Accessed 21 02 2017].

IEC, 2001. *IEC 61513:2001 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems.* [Online]
Available at: https://webstore.iec.ch/publication/19812
[Accessed 21 02 2017].

IEC, 2003. *IEC 61511-1:2003 Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements.* [Online]
Available at: https://webstore.iec.ch/publication/5522
[Accessed 21 02 2017].

IEC, 2005. *IEC 62061:2005 Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems.* [Online]
Available at: https://webstore.iec.ch/publication/6426
[Accessed 21 02 2017].

Infineon Technologies AG, 2014. *Infineon: Driving the Future of Automotive Electronics.* [Online]
Available at:
http://www.infineon.com/dgdl/Infineon+Automotive+Application+Guide+2014.pdf?fileId=5546d4614937379a01493d11ec51016b
[Accessed 05 08 2016].

ISA, 1996. *ISA 84.01:1996 Application Of Safety Instrumented Systems For The Process Industries.* [Online]
Available at: http://infostore.saiglobal.com/store/Details.aspx?productID=702949
[Accessed 21 02 2017].

Isermann R, S. R. S. S., 2002. Fault-Tolerant Drive-by-Wire Systems. *IEEE Control Systems Magazine,* 11, Volume 22(5), pp. 64-81.

ISO/DIS 26262-11, 2016. *ISO/DIS 26262-11 Road vehicles -- Functional safety -- Part 11: Guidelines on application of ISO 26262 to semiconductors,* Geneva: International Standards Organisation.

ISO, 2003. *ISO 11898-1 Road Vehicles - Controller area Network (CAN) - Part 1: Data link layer and physical signalling,* Geneva: International Organization for Standardization.

ISO, 2006. *ISO 13849-1:2006 Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design.* [Online]
Available at: https://www.iso.org/standard/34931.html
[Accessed 08 09 2018].

ISO, 2008. *ISO 15998:2008 Earth-moving machinery -- Machine-control systems (MCS) using electronic components -- Performance criteria and tests for functional safety.* [Online]
Available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=28559
[Accessed 21 02 2017].

ISO, 2010. *ISO 25119-1:2010 Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems -- Part 1: General principles for design and development.* [Online]
Available at:
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45047
[Accessed 21 02 2017].

ISO, 2013. *ISO 17458-1 Road Vehicles - FlexRay communications systm - Part 1: General information and use case definition,* Geneva: International Organization for Standardization.

Isograph, 2017. *Reliability Workbench,* warrington: Isograph Ltd.

Joshi, A. H. M. W. M., 2006. *Model-Based Safety Analysis Final Report,* Minnesota, USA: University of Minnesota Advanced Technology Center.

Karaki S, D. R. J. R. C. R. P. F., 2015. Fuel Cell Hybrid Electric Vehicle Sizing using Ordinal Optimization. *SAE Int. J. Passeng. Cars – Electron. Electr. Syst. 8(1):2015,* 14 04.

Kelly, T., 2003. *A Systematic Approach to Safety Case Management,* s.l.: Society of Automotive Engineers.

Knight, J., 2002. *Safety Critical Systems: Challenges and Directions.* Orlando, International Conference on Software Engineering.

Kunusch C, P. P. M. M., 2012. PEM Fuel Cell Systems. In: Sliding-Mode Control of PEM Fuel Cells.. *Advances in Industrial Control.*

Kurtoglu T, T. I. J. D., 2010. A Functional Failure Reasoning Method for Evaluation of Conceptual System Architectures. *Journal of Research in Engineering Design,* 10.pp. 209-234.

Lanigan P, N. P. F. T., 2010. *Experiences with a CANoe-based Fault Injection Framework for AUTOSAR.* Chicargo, IEEE.

Lanigan, P., 2011. *Diagnosis in Automotive Systems: A Survey,* Pittsburgh: Carnegie Mellon University.

Leitner-Fischer, F. & Leue, S., 2011. *The QuantUM Approach in the Context of the ISO Standard 26262 for Automotive SYstems,* Konstanz: University of Konstanz and Steinbeis Transfer Center for Complex Systems Engineering.

Leteinturier, P. B. S. a. S. K., 2008. *MultiCore Benefits & Challenges for Automotive Applications.* New York, SAE International.

Leveson, N., 2009. *Engineering a Safer World.* Massachusetts: s.n.

Linear Technology, 2010. *LTC6801 Independent Multicell Battery Stack Fault Monitor.* [Online]
Available at: http://cds.linear.com/docs/en/datasheet/6801fc.pdf
[Accessed 27 06 2017].

Linear Technology, 2011. *LTC6803-1/LTC6803-3Multicell battery Stack Monitor.* [Online]
Available at: http://cds.linear.com/docs/en/datasheet/680313fa.pdf
[Accessed 23 05 2017].

Linear Technology, 2013. *LTC6820 isoSPI Isolated Communications interface.* [Online]
[Accessed 27 07 2016].

Linear Technology, 2016. *Linear Technology LTC6804-1/LTC6804-2.* [Online]
Available at: http://cds.linear.com/docs/en/datasheet/680412fb.pdf
[Accessed 26 07 2016].

Lundteigen, M. & Rausand, M., 2006. *Assessment of Hardware Safety Integrity Requirements.* Trondheim, s.n.

Mariani R, K. T. S. H., 2007. *A flexible microcontroller architecture for fail-safe and fail-operational systems.* Rome, IEEE Computer Society.

Markel T, Z. M. W. K. P. A., 2003. *Energy Storage System Requirements for Hybrid Fuel Cell Vehicles.* Nice, France, National Renewable Energy Laboratory, pp. Battery 4,.

Mathworks, 2017. *Mathworks.* [Online]
Available at: https://uk.mathworks.com/
[Accessed 08 09 2017].

Maxim Integrated, 2014. *MAX14920-MAX14921.* [Online]
Available at: https://datasheets.maximintegrated.com/en/ds/MAX14920-MAX14921.pdf
[Accessed 26 07 2016].

Mentor Graphics, 2016. *Mentor Safe: Functonal Safety / ISO26262.* [Online]
Available at: https://www.mentor.com/solutions/automotive/subsystems-technology/functional-safety-iso26262
[Accessed 17 03 2016].

Mian, L. B. L. P. Y. B. M., 2019. System Dependability Modelling and Analysis Using AADL and HiP-HOPS. *Journal of Systems and Software.*

MISRA, 2007. *Guidelines for Safety Analysis of Vehicle based Programmable Systems.* Nuneaton: The Motor industry Software reliability Asosciation.

MOD, 2011. *An Introduction to System Safety Management in the MOD.* s.l., MOD.

NHTSA, 2008. *National Motor Vehicle Crash Causation Survey.* Virginia, USA, National Technical Information Service.

OMG SysML, 2015. *SysML Specifications - Current Version: OMG SysML 1.4.* [Online]
Available at: http://www.omg.org/spec/SysML/1.4/PDF/
[Accessed 27 01 2017].

OMG UML, 2015. *Object Management Group Unified Modelling Language.* [Online]
Available at: http://www.omg.org/spec/UML/2.5/PDF
[Accessed 27 01 2017].

OMG, 2015. *Unified Modeling Language Version 2.5.* [Online]
Available at: http://www.omg.org/spec/UML/
[Accessed 19 02 2017].

Oxford Dictionaries, 2017. *Safe definition,* s.l.: s.n.

Patton, 1989. *Fault Diagnostics in Dynamic Systems.* 1 ed. Hemel Hempstead: Prentice Hall International (UK) Ltd.

Pocock, S. H. M. W. P. J. P., 1999. *THEA: A Technique for Human Error Assessment Early in Design.* Sienna, RTO/NATO.

PRQA, 2016. *Developing Secure Embedded Software.* [Online]
Available at: http://info.programmingresearch.com/developing-secure-embedded-software-awareness-lp
[Accessed 14 03 2017].

Rama, P. C. R. a. A. J., 2008. *Failure Analysis of Polymer Electrolyte Fuel Cells.* New York, SAE International, pp. catastrophic failures 5,.

Renesas Electronics Europe, 2016. *Renesas: Chassis and Safety Applications.* [Online]
Available at: https://www.renesas.com/en-eu/doc/DocumentServer/011/R01CA0002ED0400.pdf
[Accessed 05 08 2016].

RTCA, 1992. *DO-178B Software Considerations in Airborne Systems and Equipment Certification,* Washington: Radio Technical Commission for Aeronautics.

RTCA, 2000. *DO-254 Design Assurance Guidance for Airborne Electronic Hardware,* Washington: Radio Technical Commission for Aeronautics.

RTCA, 2011. *DO-333 Formal Methods Supplement to DO-178C and DO-278A,* Washington: Radio Technical Commission for Aeronautics.

Rupanov V, K. A. F. L. A. M. S. G. B. C., 2012. *Early Safety Evaluation of design decisions in EE architecture according to ISO26262.* Bertinoro, Italy, s.n., p. 1010.

SAE, 2011. *AS5506/1 SAE Architecture Analysis and Design Language (AADL) Annex Volume 1: Annex A: Graphical AADL Notation, Annex C: AADL Meta-Model and Interchange Formats, Annex D: Language Compliance and Application Program Interface Annex E: Error Model Annex.* Warrendale, PA, USA: Socienty of Automotive Engineers.

Sharvia, A. P. Y., 2011. *Integrated Application of Compositional and Behavioural Safety Analysis.* Berlin, Springer.

Sinha, P. A. V., 2011. *Evaluation of Electric-Vehicle Architecture Alternatives.* Bangalore, IEEE.

Smith, D., 2005. *Reliability, Maintainability and Risk. Practical methods for engineers.* Seventh ed. Oxford: Butterworth-Heinemann.

Smith, D. S. K., 2004. *Functional Safety A straightforward Guide to Applying IEC 61508 and related Standards.* 2 ed. Oxford: Butterworth-Heinemann.

System Reliability Centre, 2001. *Part Failure Mode Distributions,* Rome: s.n.

Texas Instruments, 2014. *Texas Instruments: Hercules Microcontrollers.* [Online]
Available at: http://www.ti.com/lit/sg/spry185c/spry185c.pdf
[Accessed 05 08 2016].

The IET, 2015. *Position statement on Security, Safety and ISA.* [Online]
Available at: http://www.theiet.org/factfiles/isa/security-safety-page.cfm
[Accessed 27 01 2017].

The International Consortium for Fire, Safety, Health and the Environment, 2011. *Safety issues regarding fuel cell vehicles and hydrogen fueled vehicles.* [Online]
Available at: https://dps.mn.gov/divisions/sfm/document-library/Documents/Responder%20Safety/FuelCellHydrogenFuelVehicleSafety.pdf
[Accessed 05 08 2016].

TRB, 2012. *The Safety Promise and Challenge of Automotive Electronics,* Washington: Transportation Research Board.

UN ECE Reg 100, 2013. *Un ECE Reg 100; Uniform provisions concerning the approval of vehicles with regard to specific requirements for the electric power train.* E/ECE/324/Rev.2/Add.99/Rev.2-E/ECE/TRANS/505/Rev.2/Add.99/Rev.2 ed. Geneva: United Nations.

Varadarajan A, R. M. O. B. M. J., 2016. *Development and Validation of Functional Model of a Cruise control system,* s.l.: s.n.

Vector PV, 2017. *Vector PREEvision - Model-based Electric / Electronic Development,* Stuttgart: Vector Informatik GMBH.

VOSA, 2017. *Vehicle and Operator Services Agency.* [Online]
Available at: https://www.dft.gov.uk/vosa/apps/recalls/default.asp?tx
[Accessed 18 02 2017].

Walker, M. e. a., 2013. Automatic optimisation of system architectures using EAST-ADL. *Journal os Systems and Software,* pp. 2467-2887.

Ward, D., 2011. *System safety in hybrid and electric vehicles.* Nuneaton, UK, Proc. of the Australian System Safey Conference (ASSC 2011).

Ward, D., 2016. *Aligning safety and security systems for connected vehicles.* Nuneaton, Horiba Mira.

Williams, A., 2012. *Quantification of Plausibility Cross-Checks.* Gaydon, Vector UK.

Wu, W. & Kelly, T., 2006. *Deriving Safety Requirements as Part of System Architecture Definition.* Albuquerque, USA, System Safety Society.

Yu X., S. M. T. L. O. B., 2007. Fuel cell power conditioning for electric power applications: a summary. *IET Electric Power Applications,* 1(5), pp. 643-657.

8 Appendices.

Appendix A – Item Definition

This item definition is aimed at a generic vehicle level but only covers operation specifically relating to the battery management system (BMS) for a rechargeable energy storage system (RESS). As the BMS and RESS are being designed out of context for a number of vehicular applications the item definition has been purposely left all-encompassing.

The vehicle will operate in two modes:

1) Discharge mode – the normal driving mode where the RESS can be:
    a. Discharged to allow torque delivery via the driveline and ancillary power for loads such as cabin heaters, electric steering assist, electric air conditioning loads, cabin heaters etc.
    b. Charged through either regenerative braking via the driveline or in the case of a hybrid via an IC engine / generator arrangement.
2) Charge Mode – the normal charging mode where the vehicle is stationary and the RESS can be:
    a. Charged from an off board charging system. This would typically be connected to the mains distribution network and provide a DC supply to the RESS via a cable or through an inductive charging system.
    b. Charged from an on-board charger. This would typically be connected to the mains distribution network to provide and AC supply to the charger via a cable which then provides a DC supply to the RESS via the vehicle harness. Optionally an IC engine / generator arrangement may be used in the case of hybrid vehicles.
    c. Combinations of ‘a’ and ‘b’ above.

The RESS will be a DC system capable of working over a wide power range. The RESS will be tailored to suit a specific application and an impact analysis performed to assess suitability of the design prior to implementation. The voltage will range from 12VDC to 600VDC, and may either be directly referenced to the vehicle chassis or be electrically isolated from it depending upon the application. The current capability will have a maximum +/- 300ADC.

The secondary cells used within the RESS will be specific to the application and a range of different chemistries, packaging arrangements, discharge / charge ratings and environmental considerations will have to be taken into account during the design. The purpose of the BMS within the RESS is to ensure that the cells are maintained within their safe operating area during storage, transportation, installation, operation, service and up to the point of decommissioning. This safe operating area

must be specified by the vehicle manufacturer based on information from the cell manufacture and must include as a minimum the following data:

1) Maximum safe operating voltage
2) Minimum safe operating voltage
3) Maximum safe operating temperature
4) Minimum safe operating temperature
5) Maximum discharge rates - continuous and short-term
6) Maximum charge rates - continuous and short-term

If the BMS detects that the safe operating area is likely to be exceeded then it will request that the vehicle or charging system limits RESS current in order to maintain the cells within their safe operating area.

If the BMS detects that the safe operating area has been exceeded then it will request that the vehicle or charging system reduces discharge, regeneration or charge rates to zero in order to reduce switching currents and then disconnect the RESS from the vehicle / charging system.

If the vehicle or charging system detects a condition that may affect the operation of the RESS (e.g. crash) then it will request that the RESS disconnects from the vehicle or charging system.

The BMS and RESS shall connect to the vehicle and charging system through the following interface:

1) DC Bus (12VDC to 600VDC at up to 300A)
2) Logic Supply (12Vdc to 48Vdc depending on the vehicle application)
3) CAN communication to and from the vehicle and charging system. This will typically include status information such as voltages, current, temperature, State of Charge (SOC), Depth of Discharge (DOD), State of Health (SOH) and any relevant diagnostic information.
4) CAN communication using Unified Diagnostic Services (UDS) for reflash, configuration, Diagnostic Trouble Code (DTC) read / clear and data log retrieval.
5) Discrete signals for interface. This would typically include operating mode requests and enables, interlocks etc.

Appendix B – Hazard Identification

Parameter	Deviation	Consequence
Battery Voltage	Higher than safe operating region	Reduced Life of cells. Venting of gases. Chemical Burns. Fire. Explosion.
	Lower than safe operating region	Reduced Life of cells
	Connected when should be Disconnected	Electric shock. Electrocution.
	Disconnected when should be Connected	None. Inability to slow the vehicle. Loss of drive (coast).
Battery Current (Discharge)	Higher than safe operating region	Reduced Life of cells. Venting of gases. Chemical Burns. Fire. Explosion.
	Lower than safe operating region	None
Battery Current (Charge)	Higher than safe operating region	Reduced Life of cells. Venting of gases. Chemical Burns. Fire. Explosion.
	Lower than expected	None. Increased charge time. Vehicle does not charge.
	Connected when should be disconnected	Trailing charge Lead. Exposed voltage at charge outlet. Electric shock. Electrocution. Fire.
Battery temperature	Higher than safe operating region	Reduced Life of cells. Venting of gases. Chemical Burns. Fire. Explosion.
	Lower than safe operating region	None
Insulation Resistance on HV+	Lower than safe operating region	None
	Higher than safe operating region	None
Insulation Resistance on HV-	Lower than safe operating region	None
	Higher than safe operating region	None
Insulation Resistance on HV+ AND HV- simultaneously	Lower than safe operating region	Electric shock. Electrocution. Venting of gases. Chemical Burns. Fire. Explosion.

Parameter	**Deviation**	**Consequence**
	Higher than safe operating region	None
High Voltage Connection	Not Connected	None. Inability to slow the vehicle. Loss of drive (coast). Electric shock. Electrocution.
Torque	Higher than demanded	Inability to slow the vehicle. Unintended acceleration. Unintended movement from rest.
	Maximum	Sudden unintended acceleration
	Lower than demanded	Unintended deceleration
	Zero	Loss of Drive (Coast)
	Opposite sign	Pull away in wrong longitudinal direction. Change in longitudinal direction. Sudden stop and longitudinal direction change.
Power Dissipation	Higher than design intent	None. Skin Burns. Fire.
	Lower than design intent	None.

Figure B- 1: HAZOP

Appendix C - Diagnostic Coverage Techniques

The following is taken from BS ISO 26262 part 5 Annex D (BSI, 2011e) and broken down so that the detailed safety measures tables are shown below the analysed failure modes.

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
General Elements			
E.E Systems	No generic fault model available. Detailed analysis necessary.	No generic fault model available. Detailed analysis necessary.	No generic fault model available. Detailed analysis necessary.

Taken from BS ISO 26262 part 5 Annex D Table D.2 - Systems

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
Failure detection by on-line monitoring	D.2.1.1	Low	Depends on diagnostic coverage of failure detection
Comparator	D.2.1.2	High	Depends on the quality of the comparison
Majority voter	D.2.1.3	High	Depends on the quality of the voting
Dynamic principles	D.2.2.1	Medium	Depends on diagnostic coverage of failure detection
Analogue signal monitoring in preference to digital on/off states	D.2.2.2	Low	—
Self-test by software cross exchange between two independent units)	D.2.3.3	Medium	Depends on the quality of the self test

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Electrical Elements			
Relays	Does not energize or de-energize. Welded contacts	Does not energize or de-energize. Individual contacts welded	Does not energize or deenergize. Individual contacts welded
Harnesses including splice and connectors	Open Circuit Short Circuit to Ground	Open Circuit Short Circuit to Ground (d.c Coupled) Short Circuit to Vbat Short Circuit between neighbouring pins	Open Circuit Contact Resistance Short Circuit to Ground (d.c Coupled) Short Circuit to Vbat Short Circuit between neighbouring pins Resistive drift between pins

Taken from BS ISO 26262 part 5 Annex D Table D.3 – Electrical Elements

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
Failure detection by on-line monitoring	D.2.1.1	High	Depends on diagnostic coverage of failure detection

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Electrical Elements			
Sensors including signal switches	No generic fault model available. Detailed analysis necessary. Typical failure modes to be covered include	No generic fault model available. Detailed analysis necessary. Typical failure modes to be covered include Out-of-range	No generic fault model available. Detailed analysis necessary. Typical failure modes to be covered include Out-of-range

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Electrical Elements			
	Out-of-range Stuck in range	Offsets Stuck in range	Offsets Stuck in range Oscillations

Taken from BS ISO 26262 part 5 Annex D Table D.11 - Sensors

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
Failure detection by online monitoring	D.2.1.1	Low	Depends on diagnostic coverage of failure detection
Test pattern	D.2.6.1	High	—
Input comparison/voting (1oo2, 2oo3 or better redundancy)	D.2.6.5	High	Only if dataflow changes within diagnostic test interval
Sensor valid range	D.2.10.1	Low	Detects shorts to ground or power and some open circuits
Sensor correlation	D.2.10.2	High	Detects in range failures
Sensor rationality check	D.2.10.3	Medium	—

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Electrical Elements			
Final elements (actuators, lamps, buzzer, screen…)	No generic fault model available. Detailed analysis necessary.	No generic fault model available. Detailed analysis necessary.	No generic fault model available. Detailed analysis necessary.

Taken from BS ISO 26262 part 5 Annex D Table D.12 - Actuators

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
Failure detection by online monitoring	D.2.1.1	Low	Depends on diagnostic coverage of failure detection
Test pattern	D.2.6.1	High	—
Monitoring (i.e. coherence control)	D.2.11.1	High	Depends on diagnostic coverage of failure detection

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
General semiconductor elements			
Power supply	Under and over Voltage	Drift Under and over Voltage	Drift and oscillation Under and over Voltage Power spikes

Taken from BS ISO 26262 part 5 Annex D Table D.9 – Power Supply

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
Voltage or current control (input)	D.2.8.1	Low	-
Voltage or current control (input)	D.2.8.2	High	-

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
General semiconductor elements			
Clock	Stuck-at	d.c. fault model	d.c. fault model Incorrect frequency Period jitter

Taken from BS ISO 26262 part 5 Annex D Table D.10 – Program Sequencing Monitoring / Clock

Safety mechanism/measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Watchdog with separate time base without time-window	D.2.9.1	Low	-
Watchdog with separate time base and time-window	D.2.9.2	Medium	Depends on time restriction for the time-window
Logical monitoring of program sequence	D.2.9.3	Medium	Only effective against clock failures if external temporal events influence the logical program flow. Provides coverage for internal hardware failures (such as interrupt frequency errors) that can cause the software to run out of sequence
Combination of temporal and logical monitoring of program sequence	D.2.9.4	High	-
Combination of temporal and logical monitoring of program sequences with time dependency	D.2.9.5	High	Provides coverage for internal hardware failures that can cause the software to run out of sequence. When implemented with asymmetrical designs, provides coverage regarding communication sequence between main and monitoring device NOTE Method to be designed to account for execution jitter from interrupts, CPU loading, etc.

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
General semiconductor elements			
Non-volatile memory	Stuck-at for data and addresses and control interface, lines and logic	d.c. fault model for data and addresses (includes address lines within same block) and control interface, lines and logic	d.c. fault model for data, addresses (includes address lines within same block) and control interface, lines and logic

Taken from BS ISO 26262 part 5 Annex D Table D.5 – Non-Volatile Memory

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
Parity bit	D.2.5.2	Low	—
Memory monitoring using error-detection-correction codes (EDC)	D.2.4.1	High	The effectiveness depends on the number of redundant bits. Can be used to correct errors
Modified checksum	D.2.4.2	Low	Depends on the number and location of bit errors within test area
Memory Signature	D.2.4.3	High	—
Block replication	D.2.4.4	High	—

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
General semiconductor elements			
Volatile memory D.6	Stuck-at for data, addresses and control interface, lines and logic	d.c. fault model for data, addresses (includes address lines within same block and inability to write to cell) and control interface, lines and logic. Soft error model for bit cells	d.c. fault model for data, addresses (includes address lines within same block and inability to write to cell) and control interface, lines and logic Soft error model for bit cells

Taken from BS ISO 26262 part 5 Annex D Table D.6 – Volatile Memory

Safety mechanism/measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
RAM pattern test	D.2.5.1	Medium	High coverage for stuck-at failures. No coverage for linked failures. Can be appropriate to run under interrupt protection
RAM March test	D.2.5.3	High	Depends on the write read order for linked cell coverage. Test generally not appropriate for run time
Parity bit	D.2.5.2	Low	—
Memory monitoring using error-detection-correction codes (EDC)	D.2.4.1	High	The effectiveness depends on the number of redundant bits. Can be used to correct errors
Block replication	D.2.4.4	High	Common failure modes can reduce diagnostic coverage
Running checksum/CRC	D.2.5.4	High	The effectiveness of the signature depends on the polynomial in relation to the block length of the information to be protected. Care needs to be taken so that values used to determine checksum are not changed during checksum calculation Probability is 1/maximum value of checksum if random pattern is returned

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
General semiconductor elements			
Digital I/O	Stuck-at (including signal lines outside of the microcontroller)	d.c. fault model (including signal lines outside of the microcontroller)	d.c. fault model (including signal lines outside of the microcontroller) Drift and oscillation
Analogue I/O	Stuck-at (including signal lines outside of the microcontroller)	d.c. fault model (including signal lines outside of the microcontroller) Drift and oscillation	d.c. fault model (including signal lines outside of the microcontroller) Drift and oscillation

Taken from BS ISO 26262 part 5 Annex D Table D.7 – Analogue and Digital IO

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
Failure detection by online monitoring (Digital I/O)	D.2.1.1	Low	Depends on diagnostic coverage of failure detection
Test pattern	D.2.6.1	High	Depends on type of pattern
Code protection for digital I/O	D.2.6.2	Medium	Depends on type of coding
Multi-channel parallel output	D.2.6.3	High	—
Monitored outputs	D.2.6.4	High	Only if dataflow changes within diagnostic test interval
Input comparison/voting (1oo2, 2oo3 or better redundancy)	D.2.6.5	High	Only if dataflow changes within diagnostic test interval

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Specific semiconductor elements – Processing Elements			
ALU - Data Path	Stuck-at	Stuck-at at gate level	d.c. fault model Soft error model (for sequential parts)
Registers (general purpose registers bank, DMA transfer registers…), internal RAM	Stuck-at	Stuck-at at gate level Soft error model	d.c. fault model including no, wrong or multiple addressing of registers Soft error model
Address calculation (Load/Store Unit, DMA addressing logic, memory and bus interfaces)	Stuck-at	Stuck-at at gate level Soft error model (for sequential parts)	d.c. fault model including no, wrong or multiple addressing Soft error model (for sequential parts)
Interrupt handling	Omission of or continuous interrupts	Omission of or continuous interrupts Incorrect interrupt executed	Omission of or continuous Interrupts Incorrect interrupt executed Wrong priority Slow or interfered interrupt handling causing missed or delayed interrupts service
Control logic (Sequencer, coding and execution logic including flag registers and stack control)	No code execution Execution too slow Stack overflow/underflow	Wrong coding or no execution Execution too slow Stack overflow/underflow	Wrong coding, wrong or no execution Execution out of order Execution too fast or too slow Stack overflow/underflow
Configuration Registers	—	Stuck-at wrong value	Corruption of registers (soft errors) Stuck-at fault model
Other sub-elements not belonging to previous classes	Stuck-at	Stuck-at at gate level sequential part)	d.c. fault model Soft error model (for sequential part)

Taken from BS ISO 26262 part 5 Annex D Table D.4 - Processing Units

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
Self-test by software: limited number of patterns (one channel)	D.2.3.1	Medium	Depends on the quality of the self-test
Self-test by software cross exchange between two independent units	D.2.3.3	Medium	Depends of the quality of the self-test
Self-test supported by hardware (one-channel)	D.2.3.2	Medium	Depends on the quality of the self-test
Software diversified redundancy (one hardware channel)	D.2.3.4	High	Depends on the quality of the diversification. Common mode failures can reduce diagnostic coverage
Reciprocal comparison by software	D.2.3.5	High	Depends on the quality of the comparison
HW redundancy (e.g. Dual Core Lockstep, asymmetric redundancy, coded processing)	D.2.3.6	High	It depends on the quality of redundancy. Common mode failures can reduce diagnostic coverage
Configuration Register Test	D.2.3.7	High	Configuration registers only
Stack over/under flow Detection	D.2.3.8	Low	Stack boundary test only
Integrated Hardware consistency monitoring	D.2.3.9	High	Coverage for illegal hardware

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Specific semiconductor elements – Processing Elements			
Address calculation (Load/Store Unit, DMA addressing logic, memory and bus interfaces)	Stuck-at	Stuck-at at gate level Soft error model (for sequential parts)	d.c. fault model including no, wrong or multiple addressing Soft error model (for sequential parts)

Taken from BS ISO 26262 part 5 Annex D Table D.5 – Non-Volatile Memory

Safety mechanism/measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Parity bit	D.2.5.2	Low	—
Memory monitoring using error-detection-correction codes (EDC)	D.2.4.1	High	The effectiveness depends on the number of redundant bits. Can be used to correct errors
Modified checksum	D.2.4.2	Low	Depends on the number and location of bit errors within test area
Memory Signature	D.2.4.3	High	—
Block replication	D.2.4.4	High	—

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Specific semiconductor elements – Processing Elements			
Address calculation (Load/Store Unit, DMA addressing logic, memory and bus interfaces)	Stuck-at	Stuck-at at gate level Soft error model (for sequential parts)	d.c. fault model including no, wrong or multiple addressing Soft error model (for sequential parts)

Taken from BS ISO 26262 part 5 Annex D Table D.6 – Volatile Memory

Safety mechanism/measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
RAM pattern test	D.2.5.1	Medium	High coverage for stuck-at failures. No coverage for linked failures. Can be appropriate to run under interrupt protection
RAM March test	D.2.5.3	High	Depends on the write read order for linked cell

Safety mechanism/measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
			coverage. Test generally not appropriate for run time
Parity bit	D.2.5.2	Low	—
Memory monitoring using error-detection-correction codes (EDC)	D.2.4.1	High	The effectiveness depends on the number of redundant bits. Can be used to correct errors
Block replication	D.2.4.4	High	Common failure modes can reduce diagnostic coverage
Running checksum/CRC	D.2.5.4	High	The effectiveness of the signature depends on the polynomial in relation to the block length of the information to be protected. Care needs to be taken so that values used to determine checksum are not changed during checksum calculation Probability is 1/maximum value of checksum if random pattern is returned

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Specific semiconductor elements – Processing Elements			
Interrupt handling	Omission of or continuous interrupts	Omission of or continuous interrupts Incorrect interrupt executed	Omission of or continuous Interrupts. Incorrect interrupt executed. Wrong priority. Slow or interfered interrupt handling causing missed or delayed interrupts service
Control logic	No code execution	Wrong coding or no	Wrong coding, wrong or no

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Specific semiconductor elements – Processing Elements			
(Sequencer, coding and execution logic including flag registers and stack control)	Execution too slow Stack overflow/underflow	execution Execution too slow Stack overflow/underflow	execution Execution out of order Execution too fast or too slow Stack overflow/underflow

Taken from BS ISO 26262 part 5 Annex D Table D.10 – Program Sequencing Monitoring / Clock

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
Watchdog with separate time base without time-window	D.2.9.1	Low	—
Watchdog with separate time base and time window	D.2.9.2	Medium	Depends on time restriction for the time-window
Logical monitoring of program sequence	D.2.9.3	Medium	Only effective against clock failures if external temporal events influence the logical program flow. Provides coverage for internal hardware failures (such as interrupt frequency errors) that can cause the software to run out of sequence
Combination of temporal and logical monitoring of program sequence	D.2.9.4	High	—
Combination of temporal and logical monitoring of program sequences with time dependency	D.2.9.5	High	Provides coverage for internal hardware failures that can cause the software to run out of sequence. When implemented with asymmetrical designs, provides coverage regarding communication sequence between main

Safety mechanism/measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
			and monitoring device NOTE Method to be designed to account for execution jitter from interrupts, CPU loading, etc.

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Specific semiconductor elements – Processing Elements			
ALU - Data Path	Stuck-at	Stuck-at at gate level	d.c. fault model Soft error model (for sequential parts)
Other sub-elements not belonging to previous classes	Stuck-at	Stuck-at at gate level sequential part)	d.c. fault model Soft error model (for sequential part)

Taken from BS ISO 26262 part 5 Annex D Table D.13 – Combinatorial and sequential Logic

Safety mechanism/measure	See overview of techniques	Typical diagnostic coverage considered achievable	Notes
Self-test by software	D.2.3.1	Medium	—
Self-test supported by hardware (one-channel)	D.2.3.2	High	Effectiveness depends on the type of self-test. Gate level is an appropriate level for this test

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Specific semiconductor elements - Communications			
Data transmission (to be analysed with ISO 26262-6:2011, Annex D)	Failure of communication peer Message corruption Message delay Message loss Unintended message repetition	Previous + Resequencing Insertion of message	Previous + Masquerading

Taken from BS ISO 26262 part 5 Annex D Table D.8 – Communications Bus (serial, parallel)

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
One-bit hardware redundancy	D.2.7.1	Low	—
Multi-bit hardware redundancy	D.2.7.2	Medium	—
Read back of sent message	D.2.7.9	Medium	—
Complete hardware redundancy	D.2.7.3	High	Common mode failures can reduce diagnostic coverage
Inspection using test patterns	D.2.7.4	High	—
Transmission redundancy	D.2.7.5	Medium	Depends on type of redundancy. Effective only against transient faults
Information redundancy	D.2.7.6	Medium	Depends on type of redundancy
Frame counter	D.2.7.7	Medium	—
Timeout monitoring	D.2.7.8	Medium	—
Combination of information redundancy, frame counter and timeout monitoring	D.2.7.6, D.2.7.7 and D.2.7.8	High	For systems without hardware redundancy or test patterns, high coverage can be claimed for the combination of these safety mechanisms

Adapted from BS ISO 26262 part 5 Annex D Table D.1

Element	Analysed failure modes for 60%, 90% and 99% DC		
	Low (60%)	Medium (90%)	High (99%)
Specific semiconductor elements - Communications			
On-chip communication including bus-arbitration	Stuck-at (data, control, address and arbitration signals)	d.c. fault model (data, control, address and arbitration signals) Time out No or continuous arbitration	d.c. fault model (data, control, address and arbitration signals) Time out No or continuous or wrong arbitration Soft errors (for sequential part)

Taken from BS ISO 26262 part 5 Annex D Table D.14 – On-chip Communications

Safety mechanism/measure	**See overview of techniques**	**Typical diagnostic coverage considered achievable**	**Notes**
One-bit hardware redundancy	D.2.7.1	Low	—
Multi-bit hardware redundancy	D.2.7.2	Medium	Multi-bit redundancy can achieve high coverage by proper interleaving of data, address and control lines, and if combined with some complete redundancy, e.g. for the arbiter.
Complete hardware redundancy	D.2.7.3	High	Common failure modes can reduce diagnostic coverage
Test pattern	D.2.6.1	High	Depends on type of pattern

Table 80: MIR – Architecture 1 Connection 1

Reference	1)C1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262		
		Measure and Report Isolation Resistance Candidate Architecture 1								Failure Detection by on-line monitoring High 99% D.2.1.1	Used	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal				
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	0%	0%	y		➢		
				Contact resistance	10%	0%	0%	y		➢		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	0%	0%	y		➢		
			Short Circuit to Vbat	Short Circuit to Vbat	20%	0%	0%	y		➢		
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y		➢		
				Resistive drift between pins / signal lines	10%	0%	0%	y		➢		
										0.00%		

Table 81: MIR – Architecture 1 Connection 2

Reference	1)C2	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262		
		Measure and Report Isolation Resistance Candidate Architecture 1								Failure Detection by on-line monitoring High 99% D.2.1.1	Used	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal				
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	0%	0%	y		➢		
				Contact resistance	10%	0%	0%	y		➢		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	0%	0%	y		➢		
			Short Circuit to Vbat	Short Circuit to Vbat	20%	0%	0%	y		➢		
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y		➢		
				Resistive drift between pins / signal lines	10%	0%	0%	y		➢		
										0.00%		

Table 82: MIR – Architecture 1 Connection 3

Reference	1)C3	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262		
		Measure and Report Isolation Resistance Candidate Architecture 1							Failure Detection by on-line monitoring High 99% D.2.1.1	Used	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal			
		Low 60%	Medium 90%	High 99%							
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	0%	0%	y	➤		
				Contact resistance	10%	0%	0%	y	➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	0%	0%	y	➤		
			Short Circuit to Vbat	Short Circuit to Vbat	20%	0%	0%	y	➤		
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y	➤		
				Resistive drift between pins / signal lines	10%	0%	0%	y	➤		
										0.00%	

Table 83: MIR – Architecture 1 Data 1 (subset 1)

Reference	1)D1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1								Failure Detection by on-line monitoring High 99% D.2.1.1	Used	Test Pattern High 99% D.2.6.1	Used	Input Comparison Voting (1oo2, 2oo3 or better redundancy) Only if data flow chanes High 99% D.2.6.5	Used	Sensor valid range Low 60% D.2.10.1	Used	Sensor Correlation High 99% D.2.10.2	Used	Sensor rationality Check Medium 90% D.2.10.3	Used	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal												
		Low 60%	Medium 90%	High 99%																
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%	y		➤		➤		➤		➤			➤		
			Offsets	Offsets	10%	0%	0%	y		➤		➤		➤				➤			
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y		➤		➤		➤				➤			
				Oscillation	4%	0%	0%	y		➤		➤		➤				➤			
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	0%	0%	y													PCc_DATA_CHECKSUM, PCc_FRAME_COUNT, PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	0%	0%	y													PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	0%	0%	y													PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	0%	0%	y													PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	0%	0%	y													PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	0%	0%	y													PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	0%	0%	y													PCc_FRAME_COUNT
				Masquerading	1%	0%	0%	y													PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
										0.00%		0.00%		0.00%		0.00%		0.00%		0.00%	

Table 84: MIR – Architecture 1 Data 1 (subset 2)

Reference	1)D1	Failure Mode Distribution			Full Claim		PCc Claim	SG Failure Distribution	Technique Description																					Specific PCC
		100%			0.00%	Limited	0.00% Limited	100.00%	Technique from ISO26262																					
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1							Sensor rationality Check	One-bit hardware redundancy		Multi-bit hardware redundancy		Read back of sent message		Complete hardware redundancy		Inspection using test patterns		Transmission redundancy		Information redundancy		Frame counter		Timeout monitoring		Combination of information Redundancy,frame count and timeout		
									Medium 90%	Low 60%		Medium 90%		Medium 90%		High 99%		High 99%		Medium 90%		Medium 90%		Medium 90%		Medium 90%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	Used	D.2.7.1	Used	D.2.7.2	Used	D.2.7.9	Used	D.2.7.3	Used	D.2.7.4	Used	D.2.7.5	Used	D.2.7.6	Used	D.2.7.7	Used	D.2.7.8	Used	D.2.7.6,7,8	Used	
		Low 60%	Medium 90%	High 99%																										
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%	y																						
			Offsets	Offsets	10%	0%	0%	y																						
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y																						
				Oscillation	4%	0%	0%	y																						
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	0%	0%	y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_DATA_CHECKSUM, PCc_FRAME_COUNT, PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	0%	0%	y		➤		➤		➤		➤		➤		➤		➤	y	➤		➤		➤		PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	0%	0%	y		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	➤		PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	0%	0%	y		➤		➤		➤		➤		➤		➤		➤		➤	y	➤		➤		PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	0%	0%	y		➤		➤		➤		➤		➤		➤		➤		➤	y	➤		➤		PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	0%	0%	y		➤		➤		➤		➤		➤		➤		➤		➤	y	➤		➤		PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	0%	0%	y		➤		➤		➤		➤		➤		➤		➤		➤	y	➤		➤		PCc_FRAME_COUNT
				Masquerading	1%	0%	0%	y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
									####	0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		1.80%		4.50%		2.70%		15.84%		

Table 85: MIR – Architecture 1 Data 2 (subset 1)

Reference	1)D2	Failure Mode Distribution			Full Claim		PCc Claim	SG Failure Distribution	Technique Description												Specific PCC
		100%			0.00%	Limited	0.00% Limited	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1							Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		
									High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	
		Low 60%	Medium 90%	High 99%																	
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%	y	➤		➤		➤		➤				➤		
			Offsets	Offsets	10%	0%	0%	y	➤		➤		➤				➤		➤		
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y	➤		➤		➤				➤		➤		
				Oscillation	4%	0%	0%	y	➤		➤		➤				➤		➤		
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	0%	0%	y													PCc_DATA_CHECKSUM, PCc_FRAME_COUNT, PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	0%	0%	y													PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	0%	0%	y													PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	0%	0%	y													PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	0%	0%	y													PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	0%	0%	y													PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	0%	0%	y													PCc_FRAME_COUNT
				Masquerading	1%	0%	0%	y													PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		

Table 86: MIR – Architecture 1 Data 2 (subset 2)

Reference	1)D2	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description															
		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262															
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1								Sensor ration ality Check	One-bit hardware redundancy	Multi-bit hardware redundancy	Read back of sent message	Complete hardware redundancy	Inspection using test patterns	Transmission redundancy	Information redundancy	Frame counter	Timeout monitoring	Combination of information, Redundancy,f rame count and timeout	Specific PCC
										Medium 90%	Low 60%	Medium 90%	Medium 90%	High 99%	High 99%	Medium 90%	Medium 90%	Medium 90%	Medium 90%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		Used	D.2.7.1 Used	D.2.7.2 Used	D.2.7.9 Used	D.2.7.3 Used	D.2.7.4 Used	D.2.7.5 Used	D.2.7.6 Used	D.2.7.7 Used	D.2.7.8 Used	D.2.7.6,7,8 Used	
		Low	Medium	High																	
		60%	90%	99%																	
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%	y													
			Offsets	Offsets	10%	0%	0%	y													
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y													
				Oscillation	4%	0%	0%	y													
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	0%	0%	y												y	PCc_DATA_CHECKSUM, PCc_FRAME_COUNT, PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	0%	0%	y									y				PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	0%	0%	y											y		PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	0%	0%	y										y			PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	0%	0%	y										y			PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	0%	0%	y										y			PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	0%	0%	y										y			PCc_FRAME_COUNT
				Masquerading	1%	0%	0%	y												y	PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
									####		0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	1.80%	4.50%	2.70%	15.84%	

Table 87: MIR – Architecture 1 Data 4 (subset 1)

Reference	1)D4	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description															
		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262															
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1								Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Specific PCC
										High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	
		Low	Medium	High																		
		60%	90%	99%																		
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%	y														
			Offsets	Offsets	10%	0%	0%	y														
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y														
				Oscillation	4%	0%	0%	y														
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	0%	0%	y														PCc_DATA_CHECKSUM, PCc_FRAME_COUNT, PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	0%	0%	y														PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	0%	0%	y														PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	0%	0%	y														PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	0%	0%	y														PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	0%	0%	y														PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	0%	0%	y														PCc_FRAME_COUNT
				Masquerading	1%	0%	0%	y														PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
										0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		

Table 88: MIR – Architecture 1 Data 4 (subset 2)

Reference	1)D4	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1								One-bit hardware redundancy		Multi-bit hardware redundancy		Read back of sent message		Complete hardware redundancy		Inspection using test patterns		Transmission redundancy		Information redundancy		Frame counter		Timeout monitoring		Combination of information Redundancy, Frame count and timeout	
										Low		Medium		Medium		High		High		Medium		Medium		Medium		Medium		High	
										60%		90%		90%		99%		99%		90%		90%		90%		90%		99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.7.1	Used	D.2.7.2	Used	D.2.7.9	Used	D.2.7.3	Used	D.2.7.4	Used	D.2.7.5	Used	D.2.7.6	Used	D.2.7.7	Used	D.2.7.8	Used	D.2.7.6,7,8	Used	
		Low	Medium	High																										
		60%	90%	99%																										
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%	y																						
			Offsets	Offsets	10%	0%	0%	y																						
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y																						
				Oscillation	4%	0%	0%	y																						
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	0%	0%	y																				y		PCc_DATA_CHECKSUM, PCc_FRAME_COUNT, PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	0%	0%	y														y								PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	0%	0%	y																		y				PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	0%	0%	y																y						PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	0%	0%	y																y						PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	0%	0%	y																y						PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	0%	0%	y																y						PCc_FRAME_COUNT
				Masquerading	1%	0%	0%	y																				y		PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
										0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		1.80%		4.50%		2.70%		15.84%		

Table 89: MIR – Architecture 1 Data 5 (subset 1)

Reference	1)D5	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1								Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy) . Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check				
										High		High		High		Low		High		Medium				
										99%		99%		99%		60%		99%		90%				
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used			
		Low	Medium	High																				
		60%	90%	99%																				
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%	y																
			Offsets	Offsets	10%	0%	0%	y																
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y																
				Oscillation	4%	0%	0%	y																
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	0%	0%	y																PCc_DATA_CHECKSUM, PCc_FRAME_COUNT, PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	0%	0%	y																PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	0%	0%	y																PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	0%	0%	y																PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	0%	0%	y																PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	0%	0%	y																PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	0%	0%	y																PCc_FRAME_COUNT
				Masquerading	1%	0%	0%	y																PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
										0.00%		0.00%		0.00%		0.00%		0.00%		0.00%				

Table 90: MIR – Architecture 1 Data 5 (subset 2)

Reference	1)D5	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1							One-bit hardware redundancy	Multi-bit hardware redundancy	Read back of sent message	Complete hardware redundancy	Inspection using test patterns	Transmission redundancy	Information redundancy	Frame counter	Timeout monitoring	Combination of information Redundancy,Frame count and timeout	
									Low	Medium	Medium	High	High	Medium	Medium	Medium	Medium	High	
									60%	90%	90%	99%	99%	90%	90%	90%	90%	99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.7.1 Used	D.2.7.2 Used	D.2.7.9 Used	D.2.7.3 Used	D.2.7.4 Used	D.2.7.5 Used	D.2.7.6 Used	D.2.7.7 Used	D.2.7.8 Used	D.2.7.6,7,8 Used	
		Low	Medium	High															
		60%	90%	99%															
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%	y											
			Offsets	Offsets	10%	0%	0%	y											
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y											
				Oscillation	4%	0%	0%	y											
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	0%	0%	y										y	PCc_DATA_CHECKSUM, PCc_FRAME_COUNT, PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	0%	0%	y							y				PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	0%	0%	y									y		PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	0%	0%	y								y			PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	0%	0%	y								y			PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	0%	0%	y								y			PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	0%	0%	y								y			PCc_FRAME_COUNT
				Masquerading	1%	0%	0%	y										y	PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
									0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	1.80%	4.50%	2.70%	15.84%	

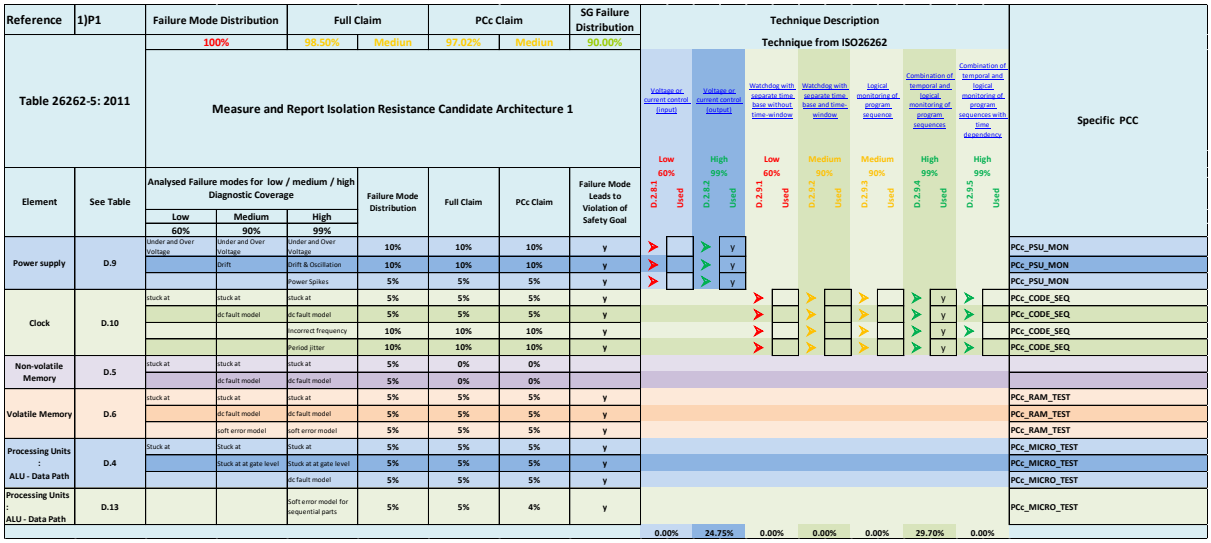
Table 91: MIR – Architecture 1 Measurement 1

Reference	1)M1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description							Specific PCC
		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262							
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1							Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	
									High	Low	High	Medium	High	High	High	
									99%	60%	99%	90%	99%	99%	99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1 Used	D.2.1.1 Used	D.2.6.1 Used	D.2.6.2 Used	D.2.6.3 Used	D.2.6.4 Used	D.2.6.5 Used	
		Low	Medium	High												
		60%	90%	99%												
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	0%	0%	y								
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	0%	0%	y								
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%	y								
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	y								
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y								
			Offsets	Offsets	15%	0%	0%	y								
		Stuck in range	Stuck in range	Stuck in range	15%	0%	0%	y								
			Drift & Oscillation	Drift & Oscillation	10%	0%	0%	y								
									0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	

Table 92: MIR – Architecture 1 Measurement 2

Reference	1)M2	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description							Specific PCC
		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262							
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1							Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	
									High	Low	High	Medium	High	High	High	
									99%	60%	99%	90%	99%	99%	99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1 Used	D.2.1.1 Used	D.2.6.1 Used	D.2.6.2 Used	D.2.6.3 Used	D.2.6.4 Used	D.2.6.5 Used	
		Low	Medium	High												
		60%	90%	99%												
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	0%	0%	y								
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	0%	0%	y								
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%	y								
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	y								
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y								
			Offsets	Offsets	15%	0%	0%	y								
		Stuck in range	Stuck in range	Stuck in range	15%	0%	0%	y								
			Drift & Oscillation	Drift & Oscillation	10%	0%	0%	y								
									0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	

Table 93: MIR – Architecture 1 Parameter 1 (subset 1)

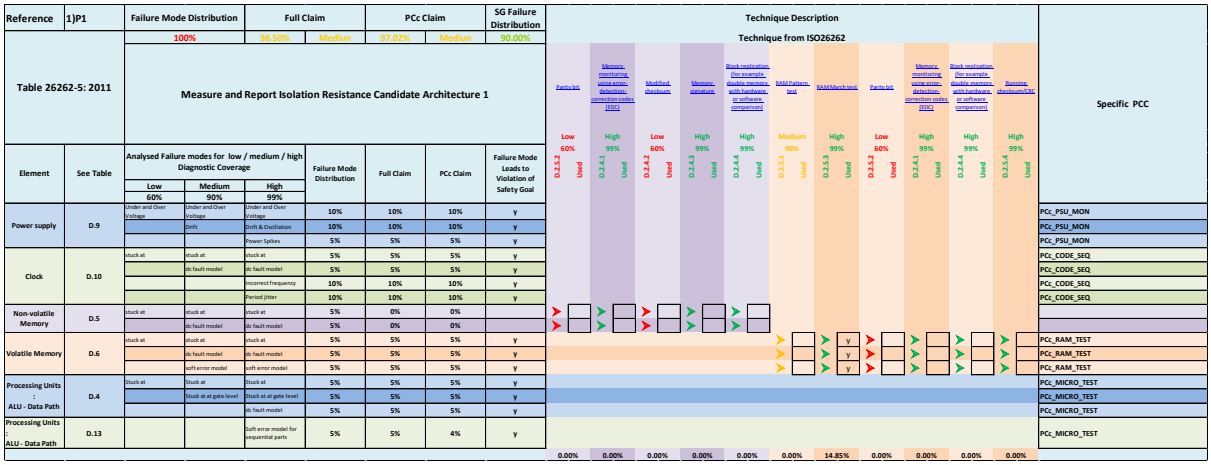


Reference	1)P1	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description
		100%	98.50%	Medium	97.02%	Medium	90.00%	Technique from ISO26262
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1						

Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	Specific PCC
		Low	Medium	High					
		60%	90%	99%					
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y	PCc_PSU_MON
			Drift	Drift & Oscillation	10%	10%	10%	y	PCc_PSU_MON
				Power Spikes	5%	5%	5%	y	PCc_PSU_MON
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y	PCc_CODE_SEQ
			dc fault model	dc fault model	5%	5%	5%	y	PCc_CODE_SEQ
				Incorrect frequency	10%	10%	10%	y	PCc_CODE_SEQ
				Period jitter	10%	10%	10%	y	PCc_CODE_SEQ
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%		
			dc fault model	dc fault model	5%	0%	0%		
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y	PCc_RAM_TEST
			dc fault model	dc fault model	5%	5%	5%	y	PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	y	PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y	PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y	PCc_MICRO_TEST
				dc fault model	5%	5%	5%	y	PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y	PCc_MICRO_TEST

Voltage or current control (input)	Voltage or current control (output)	Watchdog with separate time base without time-window	Watchdog with separate time base and time-window	Logical monitoring of program sequence	Combination of temporal and logical monitoring of program sequences	Combination of temporal and logical monitoring of program sequences with time dependency
Low 60%	High 99%	Low 60%	Medium 90%	Medium 90%	High 99%	High 99%
D.2.8.1 Used	D.2.8.2 Used	D.2.9.1 Used	D.2.9.2 Used	D.2.9.3 Used	D.2.9.4 Used	D.2.9.5 Used
0.00%	24.75%	0.00%	0.00%	0.00%	29.70%	0.00%

Table 94: MIR – Architecture 1 Parameter 1 (subset 2)

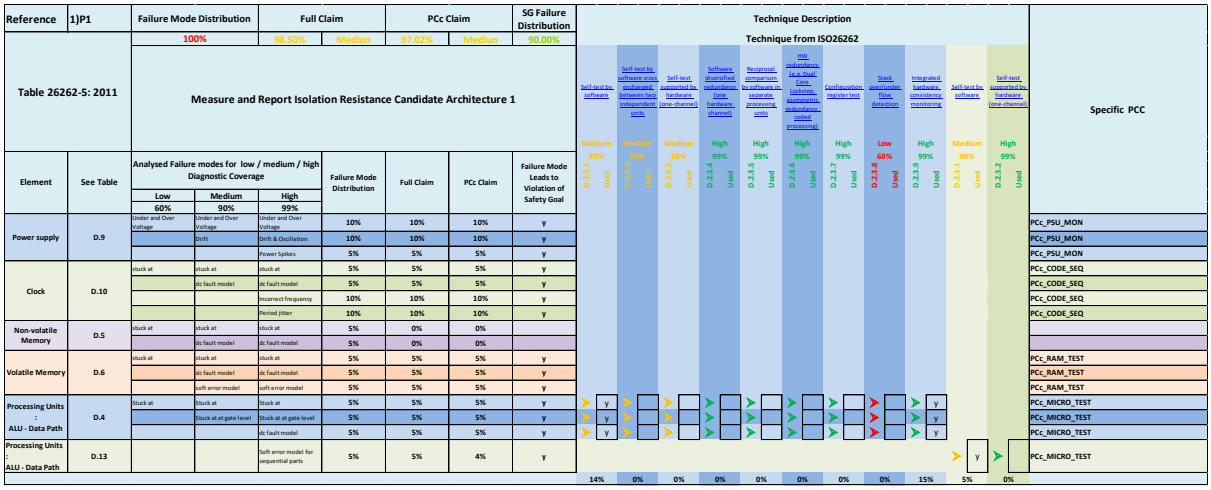


Reference	1)P1	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description
		100%	98.50%	Medium	97.02%	Medium	90.00%	Technique from ISO26262
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1						

Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	Specific PCC
		Low	Medium	High					
		60%	90%	99%					
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y	PCc_PSU_MON
			Drift	Drift & Oscillation	10%	10%	10%	y	PCc_PSU_MON
				Power Spikes	5%	5%	5%	y	PCc_PSU_MON
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y	PCc_CODE_SEQ
			dc fault model	dc fault model	5%	5%	5%	y	PCc_CODE_SEQ
				Incorrect frequency	10%	10%	10%	y	PCc_CODE_SEQ
				Period jitter	10%	10%	10%	y	PCc_CODE_SEQ
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%		
			dc fault model	dc fault model	5%	0%	0%		
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y	PCc_RAM_TEST
			dc fault model	dc fault model	5%	5%	5%	y	PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	y	PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y	PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y	PCc_MICRO_TEST
				dc fault model	5%	5%	5%	y	PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y	PCc_MICRO_TEST

Parity bit	Memory monitoring using error detection correction codes (EDC)	Modified checksum	Memory signature	Block replication (for example, double memory with hardware or software comparison)	RAM Pattern test	RAM March test	Parity bit	Memory monitoring using error detection correction codes (EDC)	Block replication (for example, double memory with hardware or software comparison)	Running checksum/CRC
Low 60%	High 99%	Low 60%	High 99%	High 99%	Medium 90%	High 99%	Low 60%	High 99%	High 99%	High 99%
D.2.3.2 Used	D.2.4.1 Used	D.2.4.2 Used	D.2.4.3 Used	D.2.4.4 Used	D.2.5.1 Used	D.2.5.3 Used	D.2.5.2 Used	D.2.4.1 Used	D.2.4.4 Used	D.2.5.4 Used
0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	14.85%	0.00%	0.00%	0.00%	0.00%

Table 95: MIR – Architecture 1 Parameter 1 (subset 3)



Reference	1)P1	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description
		100%	98.50%	Medium	97.02%	Medium	90.00%	Technique from ISO26262
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1						

Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	Specific PCC
		Low	Medium	High					
		60%	90%	99%					
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y	PCc_PSU_MON
			Drift	Drift & Oscillation	10%	10%	10%	y	PCc_PSU_MON
				Power Spikes	5%	5%	5%	y	PCc_PSU_MON
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y	PCc_CODE_SEQ
			dc fault model	dc fault model	5%	5%	5%	y	PCc_CODE_SEQ
				Incorrect frequency	10%	10%	10%	y	PCc_CODE_SEQ
				Period jitter	10%	10%	10%	y	PCc_CODE_SEQ
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%		
			dc fault model	dc fault model	5%	0%	0%		
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y	PCc_RAM_TEST
			dc fault model	dc fault model	5%	5%	5%	y	PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	y	PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y	PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y	PCc_MICRO_TEST
				dc fault model	5%	5%	5%	y	PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y	PCc_MICRO_TEST

Self-test by software	Self-test by software cross exchanged between two independent units	Self-test supported by hardware (one-channel)	Software diversified redundancy (time, hardware, channel)	Reciprocal comparison by software in separate processing units	HW redundancy (e.g. Dual Core Lockstep, asymmetric redundancy, voted processing)	Configuration register test	Stack overflow/underflow detection	Integrated hardware, consistency monitoring	Self-test by software	Self-test supported by hardware (one-channel)
Medium 90%	Medium 90%	Medium 90%	High 99%	High 99%	High 99%	High 99%	Low 60%	High 99%	Medium 90%	High 99%
D.2.3.1 Used	D.2.3.1 Used	D.2.3.2 Used	D.2.3.4 Used	D.2.3.5 Used	D.2.3.6 Used	D.2.3.7 Used	D.2.3.8 Used	D.2.3.9 Used	D.2.3.1 Used	D.2.3.2 Used
14%	0%	0%	0%	0%	0%	0%	0%	15%	5%	0%

MIR – Architecture 1 Parameter 2

Similar techniques as Architecture 1 Parameter 1 so not shown.

MIR – Architecture 1 Parameter 4

Similar techniques as Architecture 1 Parameter 1 so not shown.

MIR – Architecture 1 Parameter 6

Similar techniques as Architecture 1 Parameter 1 so not shown.

Table 96: MIR – Architecture 1 Power Supply 1

Reference	1)PSU1	Failure Mode Distribution			Full Claim	PCc Claim	Technique Description Technique from ISO26262				Specific PCC
Table D.9 26262-5: 2011		100%			99%	99%					
		Measure and Report Isolation Resistance Candidate Architecture 1					Voltage or current control (input) Low 60%		Voltage or current control (output) High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	D.2.8.1	Used	D.2.8.2	Used
		Low 60%	Medium 90%	High 99%							
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	50%	50%	49%	➤		➤	y	PCc_PSU_MON
Power supply	D.9		Drift	Drift & Oscillation	20%	20%	20%	➤		➤	y	PCc_PSU_MON
Power supply	D.9			Power Spikes	30%	30%	30%	➤		➤	y	PCc_PSU_MON
								0%		99%		

MIR – Architecture 1 Power Supply 2

Similar techniques as Architecture 1 Power Supply 1 so not shown.

Table 97: MIR – Architecture 1 Transducer 1

Reference	1)T1	Failure Mode Distribution				Full Claim		PCc Claim		SG Failure Distribution	Technique Description Technique from ISO26262										Specific PCC
		100%				0.00%	Limited	0.00%	Limited	100.00%											
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 1									Failure Detection by on-line monitoring	Test Pattern	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Sensor valid range	Sensor Correlation	Sensor rationality Check	Voltage or current control (input)	Voltage or current control (output)			
											High 99%	High 99%	High 99%	Low 60%	High 99%	Medium 90%	Low 60%	High 99%			
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal			D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.19.1	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																							
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	0%	0%	y			➤		➤		➤		➤				➤						
			Offsets	Offsets	10%	0%	0%	y			➤		➤		➤		➤		➤		➤						
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y			➤		➤		➤		➤		➤		➤						
				Oscillation	5%	0%	0%	y			➤		➤		➤		➤		➤		➤						
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	y															➤		➤		PCc_PSU_MON
			Drift	Drift & Oscillation	20%	0%	0%	y															➤		➤		PCc_PSU_MON
				Power Spikes	5%	0%	0%	y															➤		➤		PCc_PSU_MON
											0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		

Appendix D2 – MIR – Architecture 2 DC% Claims

Table 98: MIR – Architecture 2 Connection 1

Reference	2)C1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			72.00%	Low	72.00%	Low	100.00%	Technique from ISO26262		
		Measure and Report Isolation Resistance Candidate Architecture 2								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	18%	18%	y		➤	y	PCc_Ref_WIN
				Contact resistance	10%	0%	0%	y		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	27%	27%	y		➤	y	PCc_Ref_WIN
			Short Circuit to Vbat	Short Circuit to Vbat	20%	18%	18%	y		➤	y	PCc_Ref_WIN
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	9%	9%	y		➤	y	PCc_Ref_WIN
				Resistive drift between pins / signal lines	10%	0%	0%	y		➤		
										79.20%		

Table 99: MIR – Architecture 2 Connection 2

Reference	2)C2	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			72.00%	Low	72.00%	Low	100.00%	Technique from ISO26262		
		Measure and Report Isolation Resistance Candidate Architecture 2								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	18%	18%	y		➤	y	PCc_Ref_WIN
				Contact resistance	10%	0%	0%	y		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	27%	27%	y		➤	y	PCc_Ref_WIN
			Short Circuit to Vbat	Short Circuit to Vbat	20%	18%	18%	y		➤	y	PCc_Ref_WIN
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	9%	9%	y		➤	y	PCc_Ref_WIN
				Resistive drift between pins / signal lines	10%	0%	0%	y		➤		
										79.20%		

Table 100: MIR – Architecture 2 Data 1 (subset 1)

Reference	2)D1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%		98.10%	Mediun	95.89%	Mediun	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2							Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		
									High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage: Low 60%	Medium 90%	High 99%	Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	30%	29%	y	➤	y	➤		➤		➤				➤		PCc_REF_WINDOW
			Offsets	Offsets	10%	10%	10%	y	➤	y	➤		➤				➤		➤		
		Stuck in range	Stuck in range	Stuck in range	30%	30%	29%	y	➤	y	➤		➤				➤		➤		
				Oscillation	4%	4%	4%	y	➤	y	➤		➤				➤		➤		
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	15%	14%	y													PCc_DATA_CHECKSUM, PCc_FRAME_COUNT PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	2%	2%	y													PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	3%	3%	y													PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	2%	2%	y													PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	1%	1%	y													PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	1%	1%	y													PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	1%	1%	y													PCc_FRAME_COUNT
				Masquerading	1%	1%	1%	y													PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
									73.26%		0.00%		0.00%		0.00%		0.00%		0.00%		

Table 101: MIR – Architecture 2 Data 1 (subset 2)

Reference	2)D1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description																						Specific PCC
		100%		98.10%	Mediun	95.89%	Medium	100.00%	Technique from ISO26262																						
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2							Sensor rationality Check		One-bit hardware redundancy		Multi-bit hardware redundancy		Read back of sent message		Complete hardware redundancy		Inspection using test patterns		Transmission redundancy		Information redundancy		Frame counter		Timeout monitoring		Combination of information Redundancy,frame count and timeout		
									Medium 90%		Low 60%		Medium 90%		Medium 90%		High 99%		High 99%		Medium 90%		Medium 90%		Medium 90%		Medium 90%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage: Low 60%	Medium 90%	High 99%	Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.10.3	Used	D.2.7.1	Used	D.2.7.2	Used	D.2.7.9	Used	D.2.7.3	Used	D.2.7.4	Used	D.2.7.5	Used	D.2.7.6	Used	D.2.7.7	Used	D.2.7.8	Used	D.2.7.6, 7,8	Used	
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	30%	29%	y	➤																						PCc_REF_WINDOW
			Offsets	Offsets	10%	10%	10%	y	➤																						
		Stuck in range	Stuck in range	Stuck in range	30%	30%	29%	y	➤																						
				Oscillation	4%	4%	4%	y	➤																						
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	15%	14%	y			➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_DATA_CHECKSUM, PCc_FRAME_COUNT PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	2%	2%	y			➤		➤		➤		➤		➤		➤		➤	y	➤		➤		➤		PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	3%	3%	y			➤		➤		➤		➤		➤		➤		➤		➤		➤	y	➤		PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	2%	2%	y			➤		➤		➤		➤		➤		➤		➤		➤	y	➤		➤		PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	1%	1%	y			➤		➤		➤		➤		➤		➤		➤		➤	y	➤		➤		PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	1%	1%	y			➤		➤		➤		➤		➤		➤		➤		➤	y	➤		➤		PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	1%	1%	y			➤		➤		➤		➤		➤		➤		➤		➤	y	➤		➤		PCc_FRAME_COUNT
				Masquerading	1%	1%	1%	y			➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		1.80%		4.50%		2.70%		15.84%		

MIR – Architecture 2 Data 2

Similar techniques as Architecture 2 Data 1 so not shown.

MIR – Architecture 2 Data 3

Similar techniques as Architecture 2 Data 1 so not shown.

MIR – Architecture 2 Data 4

Similar techniques as Architecture 2 Data 1 so not shown.

MIR – Architecture 2 Data 5

Similar techniques as Architecture 2 Data 1 so not shown.

MIR – Architecture 2 Data 6

Similar techniques as Architecture 2 Data 1 so not shown.

Table 102: MIR – Architecture 2 Measurement 1

Reference	2)M1	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%	0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2						Failure Detection by on-line monitoring		Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		
								High 99%		Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	
		Low 60%	Medium 90%	High 99%																		
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	0%	0%	y		y													PCc_Ref_WIN
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	0%	0%	y				y											PCc_Ref_WIN
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%	y				y											PCc_Ref_WIN
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	y				y											PCc_Ref_WIN
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y				y											PCc_Ref_WIN
			Offsets	Offsets	15%	0%	0%	y															
		Stuck in range	Stuck in range	Stuck in range	15%	0%	0%	y															
			Drift & Oscillation	Drift & Oscillation	10%	0%	0%	y															
									14.85%		27.00%		0.00%		0.00%		0.00%		0.00%		0.00%		

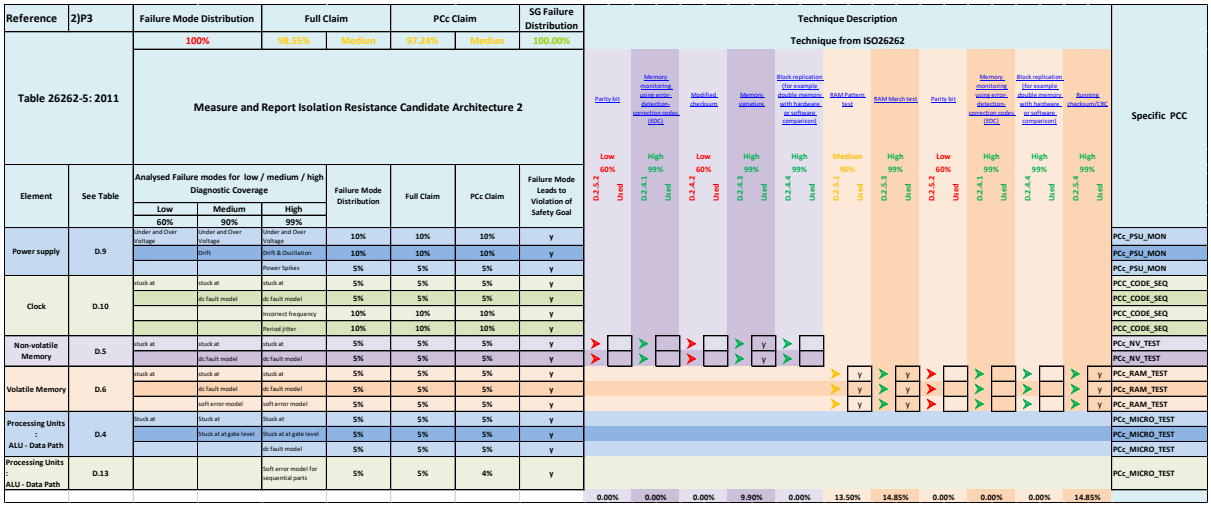
MIR – Architecture 2 Measurement 2

Similar techniques as Architecture 2 Measurement 1 so not shown.

Table 103: MIR – Architecture 2 Parameter 3 (subset 1)

Reference	2)P3	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%	98.55%	Medium	97.24%	Medium	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2						Voltage or current control (input)		Voltage or current control (output)		Watchdog with separate time base without time-window		Watchdog with separate time base and time-window		Logical monitoring of program sequence		Combination of temporal and logical monitoring of program sequences		Combination of temporal and logical monitoring of program sequences with time dependency		
								Low 60%		High 99%		Low 60%		Medium 90%		Medium 90%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.8.1	Used	D.2.8.2	Used	D.2.9.1	Used	D.2.9.2	Used	D.2.9.3	Used	D.2.9.4	Used	D.2.9.5	Used	
		Low 60%	Medium 90%	High 99%																		
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y				y											PCc_PSU_MON
			Drift	Drift & Oscillation	10%	10%	10%	y				y											PCc_PSU_MON
				Power Spikes	5%	5%	5%	y				y											PCc_PSU_MON
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y														y	PCC_CODE_SEQ
			dc fault model	dc fault model	5%	5%	5%	y														y	PCC_CODE_SEQ
				incorrect frequency	10%	10%	10%	y														y	PCC_CODE_SEQ
				Period jitter	10%	10%	10%	y														y	PCC_CODE_SEQ
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	5%	5%	y															PCc_NV_TEST
			dc fault model	dc fault model	5%	5%	5%	y															PCc_NV_TEST
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y															PCc_RAM_TEST
			dc fault model	dc fault model	5%	5%	5%	y															PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	y															PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y															PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y															PCc_MICRO_TEST
				dc fault model	5%	5%	5%	y															PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y															PCc_MICRO_TEST
									0.00%		24.75%		0.00%		0.00%		0.00%		0.00%		29.70%		

Table 104: MIR – Architecture 2 Parameter 3 (subset 2)



Reference	2)P3	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution
		100%	98.55%	Medium	97.24%	Medium	100.00%
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2					

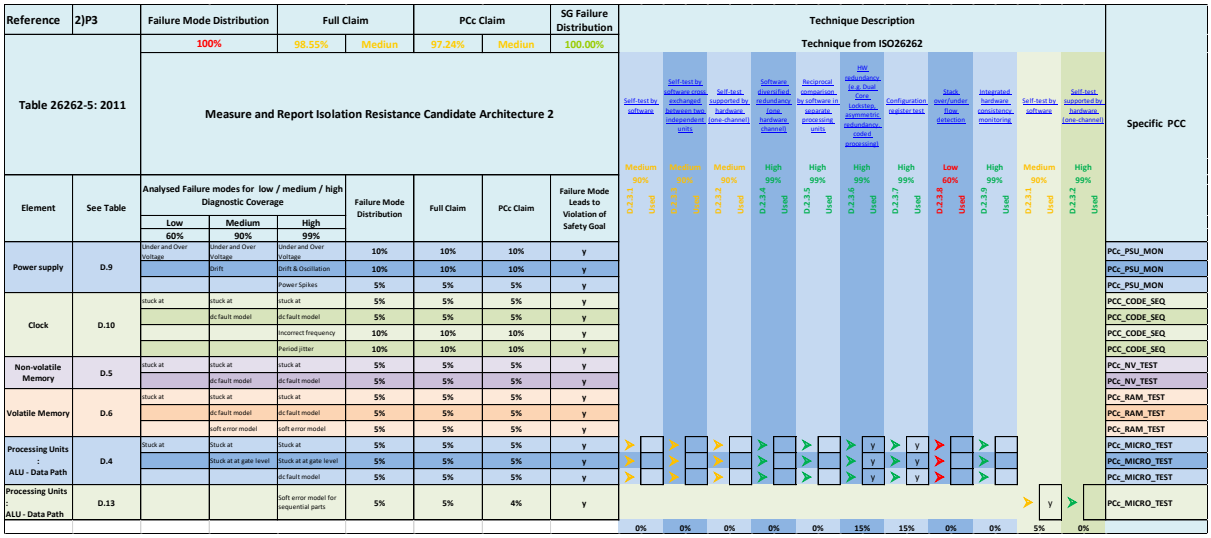
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal
		Low	Medium	High				
		60%	90%	99%				
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y
			Drift	Drift & Oscillation	10%	10%	10%	y
				Power Spikes	5%	5%	5%	y
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y
			dc fault model	dc fault model	5%	5%	5%	y
				Incorrect frequency	10%	10%	10%	y
				Period jitter	10%	10%	10%	y
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	5%	5%	y
			dc fault model	dc fault model	5%	5%	5%	y
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y
			dc fault model	dc fault model	5%	5%	5%	y
			soft error model	soft error model	5%	5%	5%	y
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y
				dc fault model	5%	5%	5%	y
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y

Technique Description

Technique from ISO26262

Parity bit	Memory monitoring using error detection correction codes (EDC)	Modified checksum	Memory signature	Block replication (for example double memory with hardware or software comparison)	RAM Pattern test	RAM March test	Parity bit	Memory monitoring using error detection correction codes (EDC)	Block replication (for example double memory with hardware or software comparison)	Running checksum/CRC	Specific PCC
Low 60% D.2.5.2 Used	High 99% D.2.4.1 Used	Low 60% D.2.4.2 Used	High 99% D.2.4.3 Used	High 99% D.2.4.4 Used	Medium 90% D.2.5.1 Used	High 99% D.2.5.3 Used	Low 60% D.2.5.2 Used	High 99% D.2.4.1 Used	High 99% D.2.4.4 Used	High 99% D.2.5.4 Used	
											PCc_PSU_MON
											PCc_PSU_MON
											PCc_PSU_MON
											PCC_CODE_SEQ
											PCC_CODE_SEQ
											PCC_CODE_SEQ
											PCC_CODE_SEQ
											PCc_NV_TEST
											PCc_NV_TEST
											PCc_RAM_TEST
											PCc_RAM_TEST
											PCc_RAM_TEST
											PCc_MICRO_TEST
											PCc_MICRO_TEST
											PCc_MICRO_TEST
0.00%	0.00%	0.00%	9.90%	0.00%	13.50%	14.85%	0.00%	0.00%	0.00%	14.85%	

Table 105: MIR – Architecture 2 Parameter 3 (subset 3)



Reference	2)P3	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution
		100%	98.55%	Medium	97.24%	Medium	100.00%
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2					

Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal
		Low	Medium	High				
		60%	90%	99%				
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y
			Drift	Drift & Oscillation	10%	10%	10%	y
				Power Spikes	5%	5%	5%	y
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y
			dc fault model	dc fault model	5%	5%	5%	y
				Incorrect frequency	10%	10%	10%	y
				Period jitter	10%	10%	10%	y
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	5%	5%	y
			dc fault model	dc fault model	5%	5%	5%	y
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y
			dc fault model	dc fault model	5%	5%	5%	y
			soft error model	soft error model	5%	5%	5%	y
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y
				dc fault model	5%	5%	5%	y
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y

Technique Description

Technique from ISO26262

Self-test by software	Self-test by software cross exchanged between two independent units	Self-test supported by hardware (one-channel)	Software diversified redundancy (one hardware channel)	Reciprocal comparison by software in separate processing units	HW redundancy (e.g. Dual Core Lockstep, asymmetric redundancy, coded processing)	Configuration register test	Stack over/under flow detection	Integrated hardware consistency monitoring	Self-test by software	Self-test supported by hardware (one-channel)	Specific PCC
Medium 90% D.2.3.1 Used	Medium 90% D.2.3.6 Used	Medium 90% D.2.3.2 Used	High 99% D.2.3.4 Used	High 99% D.2.3.5 Used	High 99% D.2.3.10 Used	High 99% D.2.3.7 Used	Low 60% D.2.3.9 Used	High 99% D.2.3.9 Used	Medium 90% D.2.3.1 Used	High 99% D.2.3.3 Used	
											PCc_PSU_MON
											PCc_PSU_MON
											PCc_PSU_MON
											PCC_CODE_SEQ
											PCC_CODE_SEQ
											PCC_CODE_SEQ
											PCC_CODE_SEQ
											PCc_NV_TEST
											PCc_NV_TEST
											PCc_RAM_TEST
											PCc_RAM_TEST
											PCc_RAM_TEST
											PCc_MICRO_TEST
											PCc_MICRO_TEST
											PCc_MICRO_TEST
											PCc_MICRO_TEST
0%	0%	0%	0%	0%	15%	15%	0%	0%	5%	0%	

MIR – Architecture 2 Parameter 5

Similar techniques as Architecture 2 Parameter 3 so not shown.

Table 106: MIR – Architecture 2 Parameter 6 (subset 1)

Reference	2)P6	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%		98.50%	Mediun	97.02%	Mediun	90.00%	Technique from ISO26262														
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2							Voltage or current control (input)		Voltage or current control (output)		Watchdog with separate time base without time-window		Watchdog with separate time base and time-window		Logical monitoring of program sequence		Combination of temporal and logical monitoring of program sequences		Combination of temporal and logical monitoring of program sequences with time dependency		
									Low 60%		High 99%		Low 60%		Medium 90%		Medium 90%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage: Low 60%	Medium 90%	High 99%	Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.8.1	Used	D.2.8.2	Used	D.2.9.1	Used	D.2.9.2	Used	D.2.9.3	Used	D.2.9.4	Used	D.2.9.5	Used	
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y	➤		➤	y											PCc_PSU_MON
			Drift	Drift & Oscillation	10%	10%	10%	y	➤		➤	y											PCc_PSU_MON
				Power Spikes	5%	5%	5%	y	➤		➤	y											PCc_PSU_MON
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y					➤		➤		➤		➤	y	➤		PCc_CODE_SEQ
			dc fault model	dc fault model	5%	5%	5%	y					➤		➤		➤		➤	y	➤		PCc_CODE_SEQ
				Incorrect frequency	10%	10%	10%	y					➤		➤		➤		➤	y	➤		PCc_CODE_SEQ
				Period jitter	10%	10%	10%	y					➤		➤		➤		➤	y	➤		PCc_CODE_SEQ
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%																
			dc fault model	dc fault model	5%	0%	0%																
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y															PCc_RAM_TEST
			dc fault model	dc fault model	5%	5%	5%	y															PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	y															PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y															PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y															PCc_MICRO_TEST
				dc fault model	5%	5%	5%	y															PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y															PCc_MICRO_TEST
									0.00%		24.75%		0.00%		0.00%		0.00%		29.70%		0.00%		

Table 107: MIR – Architecture 2 Parameter 6 (subset 2)

Reference	2)P6	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description																						Specific PCC
		100%		98.50%	Mediun	97.02%	Mediun	90.00%	Technique from ISO26262																						
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2							Parity bit		Memory monitoring using error-detection-correction codes (EDC)		Modified checksum		Memory signature		Block replication (for example double memory with hardware or software comparison)		RAM Pattern test		RAM March test		Parity bit		Memory monitoring using error-detection-correction codes (EDC)		Block replication (for example double memory with hardware or software comparison)		Running checksum/CRC		
									Low 60%		High 99%		Low 60%		High 99%		High 99%		Medium 90%		High 99%		Low 60%		High 99%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage: Low 60%	Medium 90%	High 99%	Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.5.2	Used	D.2.4.1	Used	D.2.4.2	Used	D.2.4.3	Used	D.2.4.4	Used	D.2.5.1	Used	D.2.5.3	Used	D.2.5.2	Used	D.2.4.1	Used	D.2.4.4	Used	D.2.5.4	Used	
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y																							PCc_PSU_MON
			Drift	Drift & Oscillation	10%	10%	10%	y																							PCc_PSU_MON
				Power Spikes	5%	5%	5%	y																							PCc_PSU_MON
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y																							PCc_CODE_SEQ
			dc fault model	dc fault model	5%	5%	5%	y																							PCc_CODE_SEQ
				Incorrect frequency	10%	10%	10%	y																							PCc_CODE_SEQ
				Period jitter	10%	10%	10%	y																							PCc_CODE_SEQ
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%		➤		➤		➤		➤		➤														
			dc fault model	dc fault model	5%	0%	0%		➤		➤		➤		➤		➤														
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y											➤		➤	y	➤		➤		➤		➤		PCc_RAM_TEST
			dc fault model	dc fault model	5%	5%	5%	y											➤		➤	y	➤		➤		➤		➤		PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	y											➤		➤	y	➤		➤		➤		➤		PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y																							PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y																							PCc_MICRO_TEST
				dc fault model	5%	5%	5%	y																							PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y																							PCc_MICRO_TEST
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		14.85%		0.00%		0.00%		0.00%		0.00%		

Table 108: MIR – Architecture 2 Parameter 6 (subset 3)

Reference	2)P6	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description											Specific PCC
		100%		98.50%	Mediun	97.02%	Mediun	90.00%	Technique from ISO26262											
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2							Self-test by software	Self-test by software cross exchanged between two independent units	Self-test supported by hardware (one-channel)	Software diversified redundancy (one hardware channel)	Reciprocal comparison by software in separate processing units	HW redundancy (e.g. Dual Core Lockstep, asymmetric redundancy, coded processing)	Configuration register test	Stack over/under flow detection	Integrated hardware consistency monitoring	Self-test by software	Self-test supported by hardware (one-channel)	
									Medium 90%	Medium 90%	Medium 90%	High 99%	High 99%	High 99%	High 99%	Low 60%	High 99%	Medium 90%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.3.1 Used	D.2.3.3 Used	D.2.3.2 Used	D.2.3.4 Used	D.2.3.5 Used	D.2.3.6 Used	D.2.3.7 Used	D.2.3.8 Used	D.2.3.9 Used	D.2.3.1 Used	D.2.3.2 Used	
		Low	Medium	High																
		60%	90%	99%																
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y												PCc_PSU_MON
			Drift	Drift & Oscillation	10%	10%	10%	y												PCc_PSU_MON
				Power Spikes	5%	5%	5%	y												PCc_PSU_MON
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	5%	y												PCc_CODE_SEQ
			dc fault model	dc fault model	5%	5%	5%	y												PCc_CODE_SEQ
				Incorrect frequency	10%	10%	10%	y												PCc_CODE_SEQ
				Period jitter	10%	10%	10%	y												PCc_CODE_SEQ
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%													
			dc fault model	dc fault model	5%	0%	0%													
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y												PCc_RAM_TEST
			dc fault model	dc fault model	5%	5%	5%	y												PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	y												PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y	y								y			PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y	y								y			PCc_MICRO_TEST
				dc fault model	5%	5%	5%	y	y								y			PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y										y		PCc_MICRO_TEST
									14%	0%	0%	0%	0%	0%	0%	0%	15%	5%	0%	

MIR – Architecture 2 Parameter 7

Similar techniques as Architecture 2 Parameter 6 so not shown.

MIR – Architecture 2 Parameter 8

Similar techniques as Architecture 2 Parameter 6 so not shown.

Table 109: MIR – Architecture 2 Transducer 1

Reference	2)T1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2							Failure Detection by on-line monitoring	Test Pattern	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Sensor valid range	Sensor Correlation	Sensor rationality Check	Voltage or current control (input)	Voltage or current control (output)	
									High 99%	High 99%	High 99%	Low 60%	High 99%	Medium 90%	Low 60%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1 Used	D.2.6.1 Used	D.2.6.5 Used	D.2.10.1 Used	D.2.10.2 Used	D.2.10.3 Used	D.2.8.1 Used	D.2.8.2 Used	
		Low	Medium	High													
		60%	90%	99%													
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	0%	0%	y	y			y					PCc_REF_WINDOW
			Offsets	Offsets	10%	0%	0%	y									
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y									
				Oscillation	5%	0%	0%	y									
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	y								y	PCc_PSU_MON
			Drift	Drift & Oscillation	20%	0%	0%	y								y	PCc_PSU_MON
				Power Spikes	5%	0%	0%	y								y	PCc_PSU_MON
									19.80%	0.00%	0.00%	12.00%	0.00%	0.00%	0.00%	34.65%	

Appendix D3 – MIR – Architecture 3 DC% Claims

Table 110: MIR – Architecture 3 Actuator 1

Reference	3)A1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		74.63%	Low	73.69%	Low	80.00%	Technique from ISO26262										
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 3							Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		
									Low		High		Medium		High		High		High		Low		High		
									60%		99%		90%		99%		99%		99%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																					
		60%	90%	99%																					
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	15%	9%	9%	y		y															PCc_EXT_RES_ST
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	9%	9%	y		y															PCc_EXT_RES_ST
			Short Circuit to Vbat	Short Circuit to Vbat	10%	6%	6%	y		y															PCc_EXT_RES_ST
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	6%	6%	y		y															PCc_EXT_RES_ST
			Offsets	Offsets	5%	0%	0%																		
		Stuck in range	Stuck in range	Stuck in range	10%	0%	0%																		
				Drift & Oscillation	5%	0%	0%																		
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	5%	5%	5%	y																y	PCc_PSU_MON
			Drift	Drift & Oscillation	20%	20%	20%	y																y	PCc_PSU_MON
				Power Spikes	5%	5%	5%	y																y	PCc_PSU_MON
									30.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		29.70%		

Table 111: MIR – Architecture 3 Connection 1

Reference	3)C1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			99.00%	High	99.00%	High	100.00%	Technique from ISO26262		
		Measure and Report Isolation Resistance Candidate Architecture 3								Failure Detection by on-line monitoring		
										High		
										99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used		
		Low	Medium	High								
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	20%	20%	y		y	PCc_Ref_WIN	
				Contact resistance	10%	10%	10%	y		y	PCc_ISOT_RES_ST	
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	30%	30%	y		y	PCc_Ref_WIN	
			Short Circuit to Vbat	Short Circuit to Vbat	20%	20%	20%	y		y	PCc_Ref_WIN	
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y		y	PCc_Ref_WIN	
				Resistive drift between pins / signal lines	10%	10%	10%	y		y	PCc_ISOT_RES_ST	
										99.00%		

MIR – Architecture 3 Connection 2

Similar techniques as Architecture 3 Connection 1 so not shown.

Table 112: MIR – Architecture 3 Connection 3

Reference	3)C3	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description	Specific PCC
Table 26262-5: 2011		100%		72.00%	Low	72.00%	Low	100.00%	Technique from ISO26262	
		Measure and Report Isolation Resistance Candidate Architecture 3							Failure Detection by on-line monitoring High 99% D.2.1.1 Used	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		
		Low 60%	Medium 90%	High 99%						
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	18%	18%	y	y	PCc_ISOT_RES_ST
				Contact resistance	10%	0%	0%	y		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	27%	27%	y	y	PCc_ISOT_RES_ST
			Short Circuit to Vbat	Short Circuit to Vbat	20%	18%	18%	y	y	PCc_ISOT_RES_ST
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	9%	9%	y	y	PCc_ISOT_RES_ST
				Resistive drift between pins / signal lines	10%	0%	0%	y		
									79.20%	

Table 113: MIR – Architecture 3 Data 7 (subset 1)

Reference	2)D1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
Table 26262-5: 2011		100%			98.10%	Mediun	95.89%	Mediun	100.00%	Technique from ISO26262								
		Measure and Report Isolation Resistance Candidate Architecture 2								Failure Detection by on-line monitoring High 99% D.2.1.1 Used		Test Pattern High 99% D.2.6.1 Used		Input Comparison Voting (1oo2, 2oo3 or better redundancy) Only if data flow changes within diagnostic test interval. High 99% D.2.6.5 Used		Sensor valid range Low 60% D.2.10.1 Used		Sensor Correlation High 99% D.2.10.2 Used		Sensor rationality Check Medium 90% D.2.10.3 Used		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal												
		Low 60%	Medium 90%	High 99%																
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	30%	29%	y		y										PCc_REF_WINDOW
			Offsets	Offsets	10%	10%	10%	y		y										
		Stuck in range	Stuck in range	Stuck in range	30%	30%	29%	y		y										
				Oscillation	4%	4%	4%	y		y										
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	15%	14%	y												PCc_DATA_CHECKSUM, PCc_FRAME_COUNT PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	2%	2%	y												PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	3%	3%	y												PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	2%	2%	y												PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	1%	1%	y												PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	1%	1%	y												PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	1%	1%	y												PCc_FRAME_COUNT
				Masquerading	1%	1%	1%	y												PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
										73.26%		0.00%		0.00%		0.00%		0.00%		

Table 114: MIR – Architecture 3 Data 7 (subset 2)

Reference	2)D1	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description																Specific PCC
		100%	98.10%	Medium	95.89%	Medium	100.00%	Technique from ISO26262																
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 2						Sensor rationality Check		One-bit hardware redundancy		Multi-bit hardware redundancy		Read back of sent message		Complete hardware redundancy		Inspection using test patterns		Transmission redundancy		Information redundancy		Frame counter		Timeout monitoring		Combination of information Redundancy (same count and timeout		
								Medium 90%		Low 60%		Medium 90%		Medium 90%		High 99%		High 99%		Medium 90%		Medium 90%		Medium 90%		Medium 90%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.5	Used	D.2.7.1	Used	D.2.7.2	Used	D.2.7.9	Used	D.2.7.3	Used	D.2.7.4	Used	D.2.7.5	Used	D.2.7.6	Used	D.2.7.7	Used	D.2.7.8	Used	D.2.7.6, 7,8	Used	
		Low 60%	Medium 90%	High 99%																										
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	30%	29%	y																						PCc_REF_WINDOW
			Offsets	Offsets	10%	10%	10%	y																						
		Stuck in range	Stuck in range	Stuck in range	30%	30%	29%	y																						
				Oscillation	4%	4%	4%	y																						
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	15%	14%	y																					y	PCc_DATA_CHECKSUM, PCc_FRAME_COUNT PCc_POLL_RESPONSE_TIME
		Message corruption	Message corruption	Message corruption	2%	2%	2%	y															y							PCc_DATA_CHECKSUM
		Message Delay	Message Delay	Message Delay	3%	3%	3%	y																			y			PCc_POLL_RESPONSE_TIME
		Message Loss	Message Loss	Message Loss	2%	2%	2%	y																	y					PCc_FRAME_COUNT
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	1%	1%	y																	y					PCc_FRAME_COUNT
			Resequencing	Resequencing	1%	1%	1%	y																	y					PCc_FRAME_COUNT
			Insertion of message	Insertion of message	1%	1%	1%	y																	y					PCc_FRAME_COUNT
				Masquerading	1%	1%	1%	y																					y	PCc_POLL_RESPONSE_TIME, PCc_FRAME_COUNT
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		1.80%		4.50%		2.70%		15.84%	

MIR – Architecture 3 Data 8

Similar techniques as Architecture 3 Data 7 so not shown.

Table 115: MIR – Architecture 3 Measurement 1

Reference	1)M1	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description																Specific PCC
		100%	95.10%	Medium	93.50%	Medium	100.00%	Technique from ISO26262																
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 3						Failure Detection by on-line monitoring		Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.				
								High 99%		Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%				
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used			
		Low 60%	Medium 90%	High 99%																						
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	15%	15%	y		y															PCc_Ref_WIN. PCc_ISOT_RES_ST
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	10%	10%	y														y			PCc_Ref_WIN. PCc_ISOT_RES_ST
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	15%	15%	y														y			PCc_Ref_WIN. PCc_ISOT_RES_ST
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	y														y			PCc_Ref_WIN. PCc_ISOT_RES_ST
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y														y			PCc_Ref_WIN. PCc_ISOT_RES_ST
			Offsets	Offsets	15%	15%	15%	y														y			PCc_ISOT_RES_ST
		Stuck in range	Stuck in range	Stuck in range	15%	15%	15%	y														y			PCc_ISOT_RES_ST
			Drift & Oscillation	Drift & Oscillation	10%	6%	6%	y				y													
									14.85%		6.00%		0.00%		0.00%		0.00%		74.25%		0.00%			

MIR – Architecture 3 Measurement 2

Similar techniques as Architecture 3 Measurement 1 so not shown.

Table 116: MIR – Architecture 3 Output 1

Reference	3)O1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description						Specific PCC
		100%			83.83%	Low	83.67%	Low	90.00%	Technique from ISO26262						
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 3								Failure Detection by on-line monitoring	Voltage or current control (input)	Voltage or current control (output)	Failure Detection by on-line monitoring	Test Pattern	Monitoring	
										Low 60%	Low 60%	High 99%	Low 60%	High 99%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	D.2.8.1	D.2.8.2	D.2.1.1	D.2.6.1	D.2.11.1	
		Low	Medium	High						Used	Used	Used	Used	Used	Used	
		60%	90%	99%												
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	20%	12%	12%	y		y						PCc_EXT_RES_ST
		Welded Contacts	Welded Contacts	Welded Contacts	5%	3%	3%	y		y						PCc_EXT_RES_ST
			Individual welded contacts	Individual welded contacts	10%	6%	6%	y		y						PCc_EXT_RES_ST
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y				y				PCc_PSU_MON
			Drift	Drift & Oscillation	15%	15%	15%	y				y				PCc_PSU_MON
				Power Spikes	5%	5%	5%	y				y				PCc_PSU_MON
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	10%	0%	0%									
				Incorrect action	15%	15%	15%	y					y	y	y	PCc_EXT_RES_ST
				Delayed Action	10%	10%	10%	y					y	y	y	PCc_EXT_RES_ST
										21.00%	0.00%	29.70%	15%	25%	25%	

Table 117: MIR – Architecture 3 Transducer 1

Reference	3)T1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%			85.50%	Low	84.98%	Low	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 3								Failure Detection by on-line monitoring	Test Pattern	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Sensor valid range	Sensor Correlation	Sensor rationality Check	Voltage or current control (input)	Voltage or current control (output)			
										High 99%	High 99%	High 99%	Low 60%	High 99%	Medium 90%	Low 60%	High 99%			
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	D.2.6.1	D.2.6.5	D.2.10.1	D.2.10.2	D.2.10.3	D.2.8.1	D.2.8.2			
		Low	Medium	High						Used	Used	Used	Used	Used	Used	Used	Used			
		60%	90%	99%																
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	18%	18%	y		y			y							PCc_REF_WINDOW
			Offsets	Offsets	10%	9%	9%	y		y			y	y						PCc_ISOT_RES_ST
		Stuck in range	Stuck in range	Stuck in range	30%	27%	27%	y		y			y	y						PCc_ISOT_RES_ST
				Oscillation	5%	0%	0%	y												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	9%	9%	y												PCc_PSU_MON
			Drift	Drift & Oscillation	20%	18%	18%	y												PCc_PSU_MON
				Power Spikes	5%	5%	4%	y												PCc_PSU_MON
										59.40%	0.00%	0.00%	36.00%	39.60%	0.00%	0.00%	34.65%			

Appendix D4 – MIR – Architecture 4 DC% Claims

Table 118: MIR – Architecture 4 Connection 4

Reference	4)C4	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			99.00%	High	99.00%	High	100.00%	Technique from ISO26262		
		Measure and Report Isolation Resistance Candidate Architecture 4								Failure Detection by on-line monitoring		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low	Medium	High						High 99%		
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	20%	20%	y		➢	y	PCc_EXT_RES_ST
				Contact resistance	10%	10%	10%	y		➢	y	PCc_EXT_RES_ST
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	30%	30%	y		➢	y	PCc_EXT_RES_ST
			Short Circuit to Vbat	Short Circuit to Vbat	20%	20%	20%	y		➢	y	PCc_EXT_RES_ST
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y		➢	y	PCc_EXT_RES_ST
				Resistive drift between pins / signal lines	10%	10%	10%	y		➢	y	PCc_EXT_RES_ST
										99.00%		

Table 119: MIR – Architecture 5 Measurement 1

Reference	5)M1	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%	99.00%	High	97.32%	Medium	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 5						Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		
								High 99%	Low 60%	High 99%	Medium 90%	High 99%	High 99%	High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1 Used	D.2.1.1 Used	D.2.6.1 Used	D.2.6.2 Used	D.2.6.3 Used	D.2.6.4 Used	D.2.6.5 Used	
		Low 60%	Medium 90%	High 99%												
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	15%	15%	y	y							PCc_Ref_WIN, PCc_EXT_RES_ST_TIMED
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	10%	10%	y						y		PCc_Ref_WIN, PCc_EXT_RES_ST_TIMED
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	15%	15%	y						y		PCc_Ref_WIN, PCc_EXT_RES_ST_TIMED
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	y						y		PCc_Ref_WIN, PCc_EXT_RES_ST_TIMED
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y						y		PCc_Ref_WIN, PCc_EXT_RES_ST_TIMED
			Offsets	Offsets	15%	15%	15%	y						y		PCc_EXT_RES_ST_TIMED
		Stuck in range	Stuck in range	Stuck in range	15%	15%	15%	y						y		PCc_EXT_RES_ST_TIMED
			Drift & Oscillation	Drift & Oscillation	10%	10%	10%	y						y		PCc_EXT_RES_ST_TIMED
									14.85%	0.00%	0.00%	0.00%	0.00%	84.15%	0.00%	

MIR – Architecture 5 Measurement 2

Similar techniques as Architecture 5 Measurement 1 so not shown.

Table 120: MIR – Architecture 5 Transducer 1

Reference	5)T1	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%	99.00%	High	98.33%	Medium	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Measure and Report Isolation Resistance Candidate Architecture 5						Failure Detection by on-line monitoring	Test Pattern	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Sensor valid range	Sensor Correlation	Sensor rationality Check	Voltage or current control (input)	Voltage or current control (output)			
								High 99%	High 99%	High 99%	Low 60%	High 99%	Medium 90%	Low 60%	High 99%			
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1 Used	D.2.6.1 Used	D.2.6.5 Used	D.2.10.1 Used	D.2.10.2 Used	D.2.13.1 Input	D.2.8.1 Used	D.2.8.2 Used		
		Low 60%	Medium 90%	High 99%														
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	20%	20%	y	y			y						PCc_REF_WIN, Cc_EXT_RES_ST_TIMED
			Offsets	Offsets	10%	10%	10%	y	y			y	y					PCc_EXT_RES_ST_TIMED
		Stuck in range	Stuck in range	Stuck in range	30%	30%	30%	y	y			y	y					PCc_EXT_RES_ST_TIMED
				Oscillation	5%	5%	5%	y	y									PCc_EXT_RES_ST_TIMED
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y								y		PCc_PSU_MON
			Drift	Drift & Oscillation	20%	20%	20%	y								y		PCc_PSU_MON
				Power Spikes	5%	5%	5%	y								y		PCc_PSU_MON
									64.35%	0.00%	0.00%	36.00%	39.60%	0.00%	0.00%	34.65%		

Appendix D6 – MIR – SPFM Calculation – Architecture 5

Safety Goal: Measure and Report Isolation resistance											SPFM Calculation for Architecture 5	
		Total FR (FIT)		98.438				65.655			Residual or Single Point (FIT)	1.122
											Single Point Fault Metric	98.9%
System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Failure rate distribution, %	Failure mode that can violate safety goal w/o safety mechanisms?	Failure rate based on distribution	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
	hv pos AI	J1	Y	0.0350	Short	5%	X	0.0018	SM37	EXT_RES_ST_TIMED	99%	0.0000175
					Open	59%	X	0.0207	SM37	EXT_RES_ST_TIMED	99%	0.0002065
					Value Change	36%	X	0.0126	SM37	EXT_RES_ST_TIMED	99%	0.000126
		R1	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R2	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R3	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R4	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R5	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R6	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R8	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
	hv pos AI opamp circuit	C9	Y	0.0007	Short	49%	X	0.0003	SM37	EXT_RES_ST_TIMED	99%	0.00000343
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C4	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		D1	Y	0.7100	Short	49%	X	0.3479	sm37	EXT_RES_ST_TIMED	99%	0.003479
					Open	36%		0.0000				0
					Value Change	15%		0.0000				0
		C5	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C3	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		U1D	Y	2.0000	All	50%	X	1.0000	SM37	EXT_RES_ST_TIMED	99%	0.01
					All	50%		0.0000				0
		R7	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		C54	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
	Relay Drive LED	R9	N	0.0000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		LED1	N	0.0000	Fails Off	80%		0.0000				0
					Fails On	20%		0.0000				0
	+VE Relay Drive	D3	Y	0.7200	Short	49%	X	0.3528	SM37	EXT_RES_ST_TIMED	99%	0.003528
					Open	36%	X	0.2592	SM37	EXT_RES_ST_TIMED	99%	0.002592
					Value Change	15%	X	0.1080	SM37	EXT_RES_ST_TIMED	99%	0.00108
		D9	Y	0.7100	Short	49%	X	0.3479	SM37	EXT_RES_ST_TIMED	99%	0.003479
					Open	36%	X	0.2556	SM37	EXT_RES_ST_TIMED	99%	0.002556
					Value Change	15%	X	0.1065	SM37	EXT_RES_ST_TIMED	99%	0.001065
		Q1	Y	1.2000	Short	51%	X	0.6120	SM37	EXT_RES_ST_TIMED	99%	0.00612
					Open	5%	X	0.0600	SM37	EXT_RES_ST_TIMED	99%	0.0006
					Value Change	17%	X	0.2040	SM37	EXT_RES_ST_TIMED	99%	0.00204
					Output Low	22%	X	0.2640	SM37	EXT_RES_ST_TIMED	99%	0.00264
					Output High	5%	X	0.0600	SM37	EXT_RES_ST_TIMED	99%	0.0006
		R14	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R15	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		Rly1	Y	10.0000	Fails Open	80%	X	8.0000	SM37	EXT_RES_ST_TIMED	99%	0.08
					Fails Short	20%	X	2.0000	SM37	EXT_RES_ST_TIMED	99%	0.02
		R37	N	0.0000	Short	5%		0.0000				0

System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Failure rate distribution, %	Failure mode that can violate safety goal w/o safety mechanisms?	Failure rate based on distribution	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		C43	N	0.0000	Short	49%		0.0000				0
					Open	22%		0.0000				0
	+VE Relay Feedback				Value Change	29%		0.0000				0
		D11	N	0.0000	Short	49%		0.0000				0
					Open	36%		0.0000				0
					Value Change	15%		0.0000				0
		C44	N	0.0000	Short	49%		0.0000				0
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		J2	Y	0.0350	Short	5%	X	0.0018	SM37	EXT_RES_ST_TIMED	99%	0.0000175
					Open	59%	X	0.0207	SM37	EXT_RES_ST_TIMED	99%	0.0002065
					Value Change	36%	X	0.0126	SM37	EXT_RES_ST_TIMED	99%	0.000126
		R21	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R22	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R23	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
	hv neg AI				Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R24	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R25	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R26	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R29	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		C16	Y	0.0007	Short	49%	X	0.0003	SM37	EXT_RES_ST_TIMED	99%	0.00000343
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C12	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		D5	Y	0.7100	Short	49%	X	0.3479	SM37	EXT_RES_ST_TIMED	99%	0.003479
					Open	36%		0.0000				0
					Value Change	15%		0.0000				0
		C13	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C11	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		U1A	Y	2.0000	All	50%	X	1.0000	SM37	EXT_RES_ST_TIMED	99%	0.01
					All	50%		0.0000				0
		C1	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%		0.0000				0
	hv neg AI opamp circuit				Value Change	29%		0.0000				0
		C8	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		R27	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		C10	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%	X	0.0176	SM37	EXT_RES_ST_TIMED	99%	0.000176
					Value Change	29%	X	0.0232	SM37	EXT_RES_ST_TIMED	99%	0.000232
		R19	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		U1B	Y	2.0000	All	50%	X	1.0000	SM37	EXT_RES_ST_TIMED	99%	0.01
					All	50%		0.0000				0
		R19	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		C55	Y	0.0800	Short	49%	X	0.0392	SM37	EXT_RES_ST_TIMED	99%	0.000392
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		J3	Y	0.0350	Short	5%	X	0.0018				0.00175

System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Failure rate distribution, %	Failure mode that can violate safety goal w/o safety mechanisms?	Failure rate based on distribution	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Isolation Tester	Chassis Connection				Open	59%	X	0.0207				0.02065
					Value Change	36%	X	0.0126				0.0126
	Relay Drive LED	R30	N	0.0000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		LED2	N	0.0000	Fails Off	80%		0.0000				0
					Fails On	20%		0.0000				0
	-VE Relay Drive	D7	Y	0.7200	Short	49%	X	0.3528	SM37	EXT_RES_ST_TIMED	99%	0.003528
					Open	36%	X	0.2592	SM37	EXT_RES_ST_TIMED	99%	0.002592
					Value Change	15%	X	0.1080	SM37	EXT_RES_ST_TIMED	99%	0.00108
		D10	Y	0.7100	Short	49%	X	0.3479	SM37	EXT_RES_ST_TIMED	99%	0.003479
					Open	36%	X	0.2556	SM37	EXT_RES_ST_TIMED	99%	0.002556
					Value Change	15%	X	0.1065	SM37	EXT_RES_ST_TIMED	99%	0.001065
		Q2	Y	1.2000	Short	51%	X	0.6120	SM37	EXT_RES_ST_TIMED	99%	0.00612
					Open	5%	X	0.0600	SM37	EXT_RES_ST_TIMED	99%	0.0006
					Value Change	17%	X	0.2040	SM37	EXT_RES_ST_TIMED	99%	0.00204
					Output Low	22%	X	0.2640	SM37	EXT_RES_ST_TIMED	99%	0.00264
					Output High	5%	X	0.0600	SM37	EXT_RES_ST_TIMED	99%	0.0006
		R31	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		R32	Y	0.2240	Short	5%	X	0.0112	SM37	EXT_RES_ST_TIMED	99%	0.000112
					Open	59%	X	0.1322	SM37	EXT_RES_ST_TIMED	99%	0.0013216
					Value Change	36%	X	0.0806	SM37	EXT_RES_ST_TIMED	99%	0.0008064
		Rly2	Y	10.0000	Fails Open	80%	X	8.0000	SM37	EXT_RES_ST_TIMED	99%	0.08
					Fails Short	20%	X	2.0000	SM37	EXT_RES_ST_TIMED	99%	0.02
	-VE Relay Feedback	R50	N	0.0000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		C45	N	0.0000	Short	49%		0.0000				0
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		D12	N	0.0000	Short	49%		0.0000				0
					Open	36%		0.0000				0
					Value Change	15%		0.0000				0
		C46	N	0.0000	Short	49%		0.0000				0
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
	Microcontroller	U7	Y	3.0000	All	50%	X	1.5000	SM32	MICRO_INTERNAL_ST	99%	0.0225
					All	50%		0.0000				0
		X1	Y	0.5160	Open	50%	X	0.2580	SM32	MICRO_INTERNAL_ST	99%	0.00387
					No Oscillation	50%	X	0.2580	SM32	MICRO_INTERNAL_ST	99%	0.00387
		C24	Y	0.0580	Short	49%	X	0.0284	SM32	MICRO_INTERNAL_ST	99%	0.0004263
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C28	Y	1.6800	Short	49%	X	0.8232	SM32	MICRO_INTERNAL_ST	99%	0.012348
					Open	22%	X	0.3696	SM32	MICRO_INTERNAL_ST	99%	0.005544
					Value Change	29%		0.0000				0
		C29	Y	0.0580	Short	49%	X	0.0284	SM32	MICRO_INTERNAL_ST	99%	0.0004263
					Open	22%	X	0.0128	SM32	MICRO_INTERNAL_ST	99%	0.0001914
					Value Change	29%	X	0.0168	SM32	MICRO_INTERNAL_ST	99%	0.0002523
		C30	Y	0.0580	Short	49%	X	0.0284	SM32	MICRO_INTERNAL_ST	99%	0.0004263
					Open	22%	X	0.0128	SM32	MICRO_INTERNAL_ST	99%	0.0001914
					Value Change	29%	X	0.0168	SM32	MICRO_INTERNAL_ST	99%	0.0002523
		C31	Y	0.0580	Short	49%	X	0.0284	SM32	MICRO_INTERNAL_ST	99%	0.0004263
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C32	Y	0.0580	Short	49%	X	0.0284	SM32	MICRO_INTERNAL_ST	99%	0.0002842
					Open	22%	X	0.0128	SM32	MICRO_INTERNAL_ST	99%	0.0001914
					Value Change	29%	X	0.0168	SM32	MICRO_INTERNAL_ST	99%	0.0002523
		C34	Y	0.2000	Short	49%	X	0.0980	SM32	MICRO_INTERNAL_ST	99%	0.00098
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C35	Y	0.2000	Short	49%	X	0.0980	SM32	MICRO_INTERNAL_ST	99%	0.00098
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		R35	Y	0.5160	Short	5%		0.0000				0
					Open	59%	X	0.3044	SM32	MICRO_INTERNAL_ST	99%	0.0030444
					Value Change	36%		0.0000				0
	Microcontroller Programming Header	C33	N	0.0000	Short	49%		0.0000				0
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		R34	N	0.0000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		Q5	N	0.0000	Short	51%		0.0000				0

System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Failure rate distribution, %	Failure mode that can violate safety goal w/o safety mechanisms?	Failure rate based on distribution	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
					Open	5%		0.0000				0
					Value Change	17%		0.0000				0
					Output Low	22%		0.0000				0
					Output High	5%		0.0000				0
	Fault Output	R38	N	0.0000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		R56	N	0.0000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		R58	N	0.0000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
	Fault Feedback	R62	N	0.0000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		C7	N	0.0000	Short	49%		0.0000				0
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C14	N	0.0000	Short	49%		0.0000				0
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		D4	N	0.0000	Short	49%		0.0000				0
					Open	36%		0.0000				0
					Value Change	15%		0.0000				0
	Power Supply (PSU1)	D7	Y	1.2000	Short	49%		0.0000				0
					Open	36%	X	0.4320	SM34	PSU_MON	99%	0.00432
					Value Change	15%		0.0000				0
		C18	Y	1.6800	Short	49%	X	0.8232	SM34	PSU_MON	99%	0.008232
					Open	22%	X	0.3696	SM34	PSU_MON	99%	0.003696
					Value Change	29%		0.0000				0
		C19	Y	0.0580	Short	49%	X	0.0284	SM34	PSU_MON	99%	0.0002842
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		U4	Y	1.0000	All	50%	X	0.5000	SM34	PSU_MON	99%	0.005
					All	50%		0.0000				0
		C21	Y	1.6800	Short	49%	X	0.8232	SM34	PSU_MON	99%	0.008232
					Open	22%	X	0.3696	SM34	PSU_MON	99%	0.003696
					Value Change	29%		0.0000				0
		C20	Y	0.0580	Short	49%	X	0.0284	SM34	PSU_MON	99%	0.0002842
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		U5	Y	0.4430	All	50%	X	0.2215	SM34	PSU_MON	99%	0.002215
					All	50%		0.0000				0
		C25	Y	1.6800	Short	49%	X	0.8232	SM34	PSU_MON	99%	0.008232
					Open	22%	X	0.3696	SM34	PSU_MON	99%	0.003696
					Value Change	29%		0.0000				0
		C26	Y	0.0580	Short	49%	X	0.0284	SM34	PSU_MON	99%	0.0002842
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C27	Y	1.6800	Short	49%	X	0.8232	SM34	PSU_MON	99%	0.008232
					Open	22%	X	0.3696	SM34	PSU_MON	99%	0.003696
					Value Change	29%		0.0000				0
		C22	Y	0.0580	Short	49%	X	0.0284	SM34	PSU_MON	99%	0.0002842
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		U6	Y	1.0000	All	50%	X	0.5000	SM34	PSU_MON	99%	0.005
					All	50%		0.0000				0
		C17	Y	0.0580	Short	49%	X	0.0284	SM34	PSU_MON	99%	0.0002842
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C23	Y	1.6800	Short	49%	X	0.8232	SM34	PSU_MON	99%	0.008232
					Open	22%	X	0.3696	SM34	PSU_MON	99%	0.003696
					Value Change	29%		0.0000				0
	CAN	U8	Y	0.9000	All	50%	x	0.4500	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.045
					All	50%		0.0000				0
		L1	Y	0.0017	Short	49%	x	0.0008	SM29	PCc_CAN/PCc_REF_WINDOW	90%	8.4672E-05
					Open	22%	x	0.0004	SM29	PCc_CAN/PCc_REF_WINDOW	90%	3.8016E-05
					Value Change	29%		0.0000				0
		D8	Y	2.3400	Short	49%	x	1.1466	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.11466
					Open	36%		0.0000				0
					Value Change	15%		0.0000				0
		C42	Y	0.2000	Short	49%	x	0.0980	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.0098
					Open	22%	x	0.0440	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.0044

System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Failure rate distribution, %	Failure mode that can violate safety goal w/o safety mechanisms?	Failure rate based on distribution	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
					Value Change	29%		0.0000				0
	Interface	C40	Y	0.2000	Short	49%	x	0.0980	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.0098
					Open	22%	x	0.0440	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.0044
					Value Change	29%		0.0000				0
		R40	Y	0.2240	Short	5%	x	0.0112			90%	0.00112
					Open	59%	x	0.1322			90%	0.013216
					Value Change	36%		0.0000				0
		R41	Y	0.2240	Short	5%	x	0.0112			90%	0.00112
					Open	59%	x	0.1322			90%	0.013216
					Value Change	36%		0.0000				0
		C41	Y	0.0500	Short	49%	x	0.0245	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.00245
					Open	22%	x	0.0110	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.0011
					Value Change	29%		0.0000				0
		U8	Y	0.9000	All	50%	x	0.4500	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.045
					All	50%		0.0000				0
		L1	Y	0.0017	Short	49%	x	0.0008	SM29	PCc_CAN/PCc_REF_WINDOW	90%	8.4672E-05
					Open	22%	x	0.0004	SM29	PCc_CAN/PCc_REF_WINDOW	90%	3.8016E-05
					Value Change	29%		0.0000				0
		D8	Y	2.3400	Short	49%	x	1.1466	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.11466
					Open	36%		0.0000				0
					Value Change	15%		0.0000				0
		C42	Y	0.2000	Short	49%	x	0.0980	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.0098
	CAN Interface				Open	22%	x	0.0440	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.0044
					Value Change	29%		0.0000				0
		C40	Y	0.2000	Short	49%	x	0.0980	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.0098
					Open	22%	x	0.0440	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.0044
					Value Change	29%		0.0000				0
		R40	Y	0.2240	Short	5%	x	0.0112			90%	0.00112
					Open	59%	x	0.1322			90%	0.013216
					Value Change	36%		0.0000				0
		R41	Y	0.2240	Short	5%	x	0.0112			90%	0.00112
					Open	59%	x	0.1322			90%	0.013216
					Value Change	36%		0.0000				0
		C41	Y	0.0500	Short	49%	x	0.0245	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.00245
					Open	22%	x	0.0110	SM29	PCc_CAN/PCc_REF_WINDOW	90%	0.0011
					Value Change	29%		0.0000				0
		U7	Y	3.0000	All	50%	X	1.5000	SM32	MICRO_INTERNAL_ST	99%	0.0225
					All	50%		0.0000				0
		X1	Y	0.5160	Open	50%	X	0.2580	SM32	MICRO_INTERNAL_ST	99%	0.00387
					No Oscillation	50%	X	0.2580	SM32	MICRO_INTERNAL_ST	99%	0.00387
		C24	Y	0.0580	Short	49%	X	0.0284	SM32	MICRO_INTERNAL_ST	99%	0.0004263
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C28	Y	1.6800	Short	49%	X	0.8232	SM32	MICRO_INTERNAL_ST	99%	0.012348
					Open	22%	X	0.3696	SM32	MICRO_INTERNAL_ST	99%	0.005544
					Value Change	29%		0.0000				0
		C29	Y	0.0580	Short	49%	X	0.0284	SM32	MICRO_INTERNAL_ST	99%	0.0004263
					Open	22%	X	0.0128	SM32	MICRO_INTERNAL_ST	99%	0.0001914
					Value Change	29%	X	0.0168	SM32	MICRO_INTERNAL_ST	99%	0.0002523
		C30	Y	0.0580	Short	49%	X	0.0284	SM32	MICRO_INTERNAL_ST	99%	0.0004263
					Open	22%	X	0.0128	SM32	MICRO_INTERNAL_ST	99%	0.0001914
	Microcontroller				Value Change	29%	X	0.0168	SM32	MICRO_INTERNAL_ST	99%	0.0002523
		C31	Y	0.0580	Short	49%	X	0.0284	SM32	MICRO_INTERNAL_ST	99%	0.0004263
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C32	Y	0.0580	Short	49%	X	0.0284	SM32	MICRO_INTERNAL_ST	99%	0.0002842
					Open	22%	X	0.0128	SM32	MICRO_INTERNAL_ST	99%	0.0001914
					Value Change	29%	X	0.0168	SM32	MICRO_INTERNAL_ST	99%	0.0002523
		C34	Y	0.2000	Short	49%	X	0.0980	SM32	MICRO_INTERNAL_ST	99%	0.00098
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C35	Y	0.2000	Short	49%	X	0.0980	SM32	MICRO_INTERNAL_ST	99%	0.00098
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		R35	Y	0.1100	Short	5%		0.0000				0
					Open	59%	X	0.0649	SM32	MICRO_INTERNAL_ST	99%	0.000649
					Value Change	36%		0.0000				0
		C33	N	0.0000	Short	49%		0.0000				0
	Microcontroller Programming Header				Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		R34	N	0.0000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
String		D7	Y	1.2000	Short	49%		0.0000				0

System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Failure rate distribution, %	Failure mode that can violate safety goal w/o safety mechanisms?	Failure rate based on distribution	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure mode coverage wrt violation of Safety Goal, %	Residual or Single Point failure rate/FIT
Controller	Power Supply (PSU2)				Open	36%	X	0.4320	SM34	PSU_MON	99%	0.00432
					Value Change	15%		0.0000				0
		C18	Y	1.6800	Short	49%	X	0.8232	SM34	PSU_MON	99%	0.008232
					Open	22%	X	0.3696	SM34	PSU_MON	99%	0.003696
					Value Change	29%		0.0000				0
		C19	Y	0.0580	Short	49%	X	0.0284	SM34	PSU_MON	99%	0.0002842
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		U4	Y	1.0000	All	50%	X	0.5000	SM34	PSU_MON	99%	0.005
					All	50%		0.0000				0
		C21	Y	1.6800	Short	49%	X	0.8232	SM34	PSU_MON	99%	0.008232
					Open	22%	X	0.3696	SM34	PSU_MON	99%	0.003696
					Value Change	29%		0.0000				0
		C20	Y	0.0580	Short	49%	X	0.0284	SM34	PSU_MON	99%	0.0002842
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		U5	Y	0.4430	All	50%	X	0.2215	SM34	PSU_MON	99%	0.002215
					All	50%		0.0000				0
		C25	Y	1.6800	Short	49%	X	0.8232	SM34	PSU_MON	99%	0.008232
					Open	22%	X	0.3696	SM34	PSU_MON	99%	0.003696
					Value Change	29%		0.0000				0
		C26	Y	0.0580	Short	49%	X	0.0284	SM34	PSU_MON	99%	0.0002842
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C27	Y	1.6800	Short	49%	X	0.8232	SM34	PSU_MON	99%	0.008232
					Open	22%	X	0.3696	SM34	PSU_MON	99%	0.003696
					Value Change	29%		0.0000				0
		C22	Y	0.0580	Short	49%	X	0.0284	SM34	PSU_MON	99%	0.0002842
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		U6	Y	1.0000	All	50%	X	0.5000	SM34	PSU_MON	99%	0.005
					All	50%		0.0000				0
		C17	Y	0.0580	Short	49%	X	0.0284	SM34	PSU_MON	99%	0.0002842
					Open	22%		0.0000				0
					Value Change	29%		0.0000				0
		C23	Y	1.6800	Short	49%	X	0.8232	SM34	PSU_MON	99%	0.008232
					Open	22%	X	0.3696	SM34	PSU_MON	99%	0.003696
					Value Change	29%		0.0000				0
	Test Res & Driver	R87	Y	0.5000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		R88	Y	0.5000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		R91	Y	0.5000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		Opt04	Y	1.8000	Short	31%	X	0.5580	SM37	EXT_RES_ST_TIMED	99%	0.00558
					Open	25%		0.0000				0
					Value Change	17%		0.0000				0
					Output Low	22%	X	0.3960	SM37	EXT_RES_ST_TIMED	99%	0.00396
					Output High	5%		0.0000				0
		Rly2	Y	10.0000	Fails Open	80%		0.0000				0
					Fails Short	20%	X	2.0000	SM37	EXT_RES_ST_TIMED	99%	0.02
		Q6	Y	1.2000	Short	51%	X	0.6120	SM37	EXT_RES_ST_TIMED	99%	0.00612
					Open	5%		0.0000				0
					Value Change	17%		0.0000				0
					Output Low	22%		0.0000				0
					Output High	5%	X	0.0600	SM37	EXT_RES_ST_TIMED	99%	0.0006
		R89	N	0.0000	Short	5%		0.0000				0
					Open	59%		0.0000				0
					Value Change	36%		0.0000				0
		LED2	N	0.0000	Fails Off	80%		0.0000				0
					Fails On	20%		0.0000				0

Safety Goal: Measure and Report Isolation resistance — LFM Calculation for Architecture 5

Total FR (FIT): 98.438 — Multi Point (FIT): 5.280

Latent Fault Metric: 91.8%

System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent		Reference	Failure Mode coverage with respect to Latent failures, %	Latent multiple-Point failure rate/FIT
	hv pos AI	J1	Y	0.0350	Short	0.001733	Y	100%	SC_EXT_REF			99%	0.0000
					Open	0.020444	Y	100%	SC_EXT_REF			99%	0.0002
					Value Change	0.012474	Y	100%	SC_EXT_REF			99%	0.0001
		R1	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF			99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF			99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF			99%	0.0008
		R2	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF			99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF			99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF			99%	0.0008
		R3	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF			99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF			99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF			99%	0.0008
		R4	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF			99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF			99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF			99%	0.0008
		R5	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF			99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF			99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF			99%	0.0008
		R6	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF			99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF			99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF			99%	0.0008
		R8	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF			99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF			99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF			99%	0.0008
	hv pos AI opamp circuit	C9	Y	0.0007	Short	0.000340	Y	100%	SC_EXT_REF			99%	0.0000
					Open	0.000154							
					Value Change	0.000203							
		C4	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF			99%	0.0004
					Open	0.017600							
					Value Change	0.023200							
		D1	Y	0.7100	Short	0.344421							
					Open	0.255600							
					Value Change	0.106500							
		C5	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF			99%	0.0004
					Open	0.017600							
					Value Change	0.023200							
		C3	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF			99%	0.0004
					Open	0.017600							
					Value Change	0.023200							
		U1D	Y	2.0000	All	0.990000	Y	100%	SC_EXT_REF			99%	0.0099
					All	1.000000							
		R7	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF			99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF			99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF			99%	0.0008
		C54	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF			99%	0.0004
					Open	0.017600							
					Value Change	0.023200							
	Relay Drive LED	R9	N	0.0000	Short	0.000000							
					Open	0.000000							
					Value Change	0.000000							
		LED1	N	0.0000	Fails Off	0.000000							
					Fails On	0.000000							
	+VE Relay Drive	D3	Y	0.7200	Short	0.349272	Y	100%	SC_EXT_REF			99%	0.0035
					Open	0.256608	Y	100%	SC_EXT_REF			99%	0.0026
					Value Change	0.106920	Y	100%	SC_EXT_REF			99%	0.0011
		D9	Y	0.7100	Short	0.344421	Y	100%	SC_EXT_REF			99%	0.0034
					Open	0.253044	Y	100%	SC_EXT_REF			99%	0.0025
					Value Change	0.105435	Y	100%	SC_EXT_REF			99%	0.0011
		Q1	Y	1.2000	Short	0.605880	Y	100%	SC_EXT_REF			99%	0.0061
					Open	0.059400	Y	100%	SC_EXT_REF			99%	0.0006
					Value Change	0.201960	Y	100%	SC_EXT_REF			99%	0.0020
					Output Low	0.261360	Y	100%	SC_EXT_REF			99%	0.0026
					Output High	0.059400	Y	100%	SC_EXT_REF			99%	0.0006
		R14	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF			99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF			99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF			99%	0.0008
		R15	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF			99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF			99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF			99%	0.0008
		Rly1	Y	10.0000	Fails Open	7.920000	Y	100%	SC_EXT_REF			99%	0.0792
					Fails Short	1.980000	Y	100%	SC_EXT_REF			99%	0.0198
		R37	N	0.0000	Short	0.000000							

MRIR LFM Calculation Page 1 of 6

System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %	Detection mean? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode coverage with respect to Latent failures, %	Latent multiple-Point failure rate/FIT
					Open	0.000000						
					Value Change	0.000000						
		C43	N	0.0000	Short	0.000000						
					Open	0.000000						
	+VE Relay Feedback				Value Change	0.000000						
		D11	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		C44	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		J2	Y	0.0350	Short	0.001733	Y	100%	SC_EXT_REF		99%	0.0000
					Open	0.020444	Y	100%	SC_EXT_REF		99%	0.0002
					Value Change	0.012474	Y	100%	SC_EXT_REF		99%	0.0001
		R21	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		R22	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		R23	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
	hv neg AI				Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		R24	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		R25	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		R26	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		R29	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		C16	Y	0.0007	Short	0.000340	Y	100%	SC_EXT_REF		99%	0.0000
					Open	0.000154						
					Value Change	0.000203						
		C12	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF		99%	0.0004
					Open	0.017600						
					Value Change	0.023200						
		D5	Y	0.7100	Short	0.344421						
					Open	0.255600						
					Value Change	0.106500						
		C13	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF		99%	0.0004
					Open	0.017600						
					Value Change	0.023200						
		C11	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF		99%	0.0004
					Open	0.017600						
					Value Change	0.023200						
		U1A	Y	2.0000	All	0.990000	Y	100%	SC_EXT_REF		99%	0.0099
					All	1.000000						
		C1	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF		99%	0.0004
					Open	0.017600						
	hv neg AI opamp circuit				Value Change	0.023200						
		C8	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF		99%	0.0004
					Open	0.017600						
					Value Change	0.023200						
		R27	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		C10	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF		99%	0.0004
					Open	0.017424	Y	100%	SC_EXT_REF		99%	0.0002
					Value Change	0.022968	Y	100%	SC_EXT_REF		99%	0.0002
		R19	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		U1B	Y	2.0000	All	0.990000	Y	100%	SC_EXT_REF		99%	0.0099
					All	1.000000						
		R19	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		C55	Y	0.0800	Short	0.038808	Y	100%	SC_EXT_REF		99%	0.0004
					Open	0.017600						
					Value Change	0.023200						
		J3	Y	0.0350	Short	0.000000	Y	100%	SC_EXT_REF		99%	0.0000

System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode coverage with respect to Latent failures, %	Latent multiple Point failure rate/FIT
Isolation Tester	Chassis Connection				Open	0.000000	Y	100%	SC_EXT_REF		99%	0.0000
					Value Change	0.000000	Y	100%	SC_EXT_REF		99%	0.0000
	Relay Drive LED	R30	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		LED2	N	0.0000	Fails Off	0.000000						
					Fails On	0.000000						
	-VE Relay Drive	D7	Y	0.7200	Short	0.349272	Y	100%	SC_EXT_REF		99%	0.0035
					Open	0.256608	Y	100%	SC_EXT_REF		99%	0.0026
					Value Change	0.106920	Y	100%	SC_EXT_REF		99%	0.0011
		D10	Y	0.7100	Short	0.344421	Y	100%	SC_EXT_REF		99%	0.0034
					Open	0.253044	Y	100%	SC_EXT_REF		99%	0.0025
					Value Change	0.105435	Y	100%	SC_EXT_REF		99%	0.0011
		Q2	Y	1.2000	Short	0.605880	Y	100%	SC_EXT_REF		99%	0.0061
					Open	0.059400	Y	100%	SC_EXT_REF		99%	0.0006
					Value Change	0.201960	Y	100%	SC_EXT_REF		99%	0.0020
					Output Low	0.261360	Y	100%	SC_EXT_REF		99%	0.0026
					Output High	0.059400	Y	100%	SC_EXT_REF		99%	0.0006
		R31	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		R32	Y	0.2240	Short	0.011088	Y	100%	SC_EXT_REF		99%	0.0001
					Open	0.130838	Y	100%	SC_EXT_REF		99%	0.0013
					Value Change	0.079834	Y	100%	SC_EXT_REF		99%	0.0008
		Rly2	Y	10.0000	Fails Open	7.920000	Y	100%	SC_EXT_REF		99%	0.0792
					Fails Short	1.980000	Y	100%	SC_EXT_REF		99%	0.0198
	-VE Relay Feedback	R50	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		C45	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		D12	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		C46	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
	Microcontroller	U7	Y	3.0000	All	1.477500	Y	100%	WDOG_EXT_MON	SM5	80%	0.2955
					All	1.500000						
		X1	Y	0.5160	Open	0.254130	Y	100%	WDOG_EXT_MON	SM5	80%	0.050826
					No Oscillation	0.254130	Y	100%	WDOG_EXT_MON	SM5	80%	0.050826
		C24	Y	0.0580	Short	0.027994	Y	100%	WDOG_EXT_MON	SM5	80%	0.005599
					Open	0.012760						
					Value Change	0.016820	Y	100%	WDOG_EXT_MON	SM5	80%	0.003364
		C28	Y	1.6800	Short	0.810852	Y	100%	WDOG_EXT_MON	SM5	80%	0.16217
					Open	0.364056	Y	100%	WDOG_EXT_MON	SM5	80%	0.072811
					Value Change	0.487200						
		C29	Y	0.0580	Short	0.027994	Y	100%	WDOG_EXT_MON	SM5	80%	0.005599
					Open	0.012569	Y	100%	WDOG_EXT_MON	SM5	80%	0.002514
					Value Change	0.016568	Y	100%	WDOG_EXT_MON	SM5	80%	0.003314
		C30	Y	0.0580	Short	0.027994	Y	100%	WDOG_EXT_MON	SM5	80%	0.005599
					Open	0.012569	Y	100%	WDOG_EXT_MON	SM5	80%	0.002514
					Value Change	0.016568	Y	100%	WDOG_EXT_MON	SM5	80%	0.003314
		C31	Y	0.0580	Short	0.027994	Y	100%	WDOG_EXT_MON	SM5	80%	0.005599
					Open	0.012760						
					Value Change	0.016820						
		C32	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SM5	80%	0.005627
					Open	0.012569	Y	100%	WDOG_EXT_MON	SM5	80%	0.002514
					Value Change	0.016568	Y	100%	WDOG_EXT_MON	SM5	80%	0.003314
		C34	Y	0.2000	Short	0.097020	Y	100%	WDOG_EXT_MON	SM5	80%	0.019404
					Open	0.044000						
					Value Change	0.058000						
		C35	Y	0.2000	Short	0.097020	Y	100%	WDOG_EXT_MON	SM5	80%	0.019404
					Open	0.044000						
					Value Change	0.058000	Y	100%	WDOG_EXT_MON	SM5	80%	0.0116
		R35	Y	0.5160	Short	0.025800						
					Open	0.301396	Y	100%	WDOG_EXT_MON	SM5	80%	0.060279
					Value Change	0.185760						
	Microcontroller Programming Header	C33	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		R34	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		Q5	N	0.0000	Short	0.000000						

System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode coverage with respect to Latent failures, %	Latent multiple-Point failure rate/FIT
					Open	0.000000						
					Value Change	0.000000						
					Output Low	0.000000						
					Output High	0.000000						
	Fault Output	R38	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		R56	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		R58	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
	Fault Feedback	R62	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		C7	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		C14	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		D4	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
	Power Supply (PSU1)	D7	Y	1.2000	Short	0.588000						
					Open	0.427680	Y	100%	WDOG_EXT_MON	SMS	80%	0.085536
					Value Change	0.180000						
		C18	Y	1.6800	Short	0.814968	Y	100%	WDOG_EXT_MON	SMS	80%	0.162994
					Open	0.365904	Y	100%	WDOG_EXT_MON	SMS	80%	0.073181
					Value Change	0.487200						
		C19	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SMS	80%	0.005627
					Open	0.012760						
					Value Change	0.016820						
		U4	Y	1.0000	All	0.495000	Y	100%	WDOG_EXT_MON	SMS	80%	0.099
					All	0.500000						
		C21	Y	1.6800	Short	0.814968	Y	100%	WDOG_EXT_MON	SMS	80%	0.162994
					Open	0.365904	Y	100%	WDOG_EXT_MON	SMS	80%	0.073181
					Value Change	0.487200						
		C20	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SMS	80%	0.005627
					Open	0.012760						
					Value Change	0.016820						
		U5	Y	0.4430	All	0.219285	Y	100%	WDOG_EXT_MON	SMS	80%	0.043857
					All	0.221500						
		C25	Y	1.6800	Short	0.814968	Y	100%	WDOG_EXT_MON	SMS	80%	0.162994
					Open	0.365904	Y	100%	WDOG_EXT_MON	SMS	80%	0.073181
					Value Change	0.487200						
		C26	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SMS	80%	0.005627
					Open	0.012760						
					Value Change	0.016820						
		C27	Y	1.6800	Short	0.814968	Y	100%	WDOG_EXT_MON	SMS	80%	0.162994
					Open	0.365904	Y	100%	WDOG_EXT_MON	SMS	80%	0.073181
					Value Change	0.487200						
		C22	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SMS	80%	0.005627
					Open	0.012760						
					Value Change	0.016820						
		U6	Y	1.0000	All	0.495000	Y	100%	WDOG_EXT_MON	SMS	80%	0.099
					All	0.500000						
		C17	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SMS	80%	0.005627
					Open	0.012760						
					Value Change	0.016820						
		C23	Y	1.6800	Short	0.814968	Y	100%	WDOG_EXT_MON	SMS	80%	0.162994
					Open	0.365904	Y	100%	WDOG_EXT_MON	SMS	80%	0.073181
					Value Change	0.487200						
	CAN	U8	Y	0.9000	All	0.405000						
					All	0.450000						
		L1	Y	0.0017	Short	0.000762						
					Open	0.000342						
					Value Change	0.000501						
		D8	Y	2.3400	Short	1.031940						
					Open	0.842400	Y	100%	WDOG_EXT_MON	SMS	80%	0.16848
					Value Change	0.351000						
		C42	Y	0.2000	Short	0.088200						
					Open	0.039600						

System	Sub-system	Component name	Safety Critical component	Safety Critical Failure rate	Failure Mode	Multiple Point Failure rate (Perceived + Latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode coverage with respect to Latent failures, %	Latent multiple-Point failure rate/FIT
	CAN Interface				Value Change	0.058000						
		C40	Y	0.2000	Short	0.088200						
					Open	0.039600						
					Value Change	0.058000						
		R40	Y	0.2240	Short	0.010080						
					Open	0.118944						
					Value Change	0.080640						
		R41	Y	0.2240	Short	0.010080						
					Open	0.118944						
					Value Change	0.080640						
		C41	Y	0.0500	Short	0.022050						
					Open	0.009900						
					Value Change	0.014500						
		U8	Y	0.9000	All	0.405000						
					All	0.450000						
		L1	Y	0.0017	Short	0.000762						
					Open	0.000342						
					Value Change	0.000501						
		D8	Y	2.3400	Short	1.031940						
					Open	0.842400	Y	100%	WDOG_EXT_MON	SM9	80%	0.16848
					Value Change	0.351000						
		C42	Y	0.2000	Short	0.088200						
					Open	0.039600						
					Value Change	0.058000						
		C40	Y	0.2000	Short	0.088200						
					Open	0.039600						
					Value Change	0.058000						
		R40	Y	0.2240	Short	0.010080						
					Open	0.118944						
					Value Change	0.080640						
		R41	Y	0.2240	Short	0.010080						
					Open	0.118944						
					Value Change	0.080640						
		C41	Y	0.0500	Short	0.022050						
					Open	0.009900						
					Value Change	0.014500						
	Microcontroller	U7	Y	3.0000	All	1.477500	Y	100%	WDOG_EXT_MON	SM9	80%	0.2955
					All	1.500000						
		X1	Y	0.5160	Open	0.254130	Y	100%	WDOG_EXT_MON	SM9	80%	0.050826
					No Oscillation	0.254130	Y	100%	WDOG_EXT_MON	SM9	80%	0.050826
		C24	Y	0.0580	Short	0.027994	Y	100%	WDOG_EXT_MON	SM9	80%	0.005599
					Open	0.012760						
					Value Change	0.016820	Y	100%	WDOG_EXT_MON	SM9	80%	0.003364
		C28	Y	1.6800	Short	0.810852	Y	100%	WDOG_EXT_MON	SM9	80%	0.16217
					Open	0.364056	Y	100%	WDOG_EXT_MON	SM9	80%	0.072811
					Value Change	0.487200						
		C29	Y	0.0580	Short	0.027994	Y	100%	WDOG_EXT_MON	SM9	80%	0.005599
					Open	0.012569	Y	100%	WDOG_EXT_MON	SM9	80%	0.002514
					Value Change	0.016568	Y	100%	WDOG_EXT_MON	SM9	80%	0.003314
		C30	Y	0.0580	Short	0.027994	Y	100%	WDOG_EXT_MON	SM9	80%	0.005599
					Open	0.012569	Y	100%	WDOG_EXT_MON	SM9	80%	0.002514
					Value Change	0.016568	Y	100%	WDOG_EXT_MON	SM9	80%	0.003314
		C31	Y	0.0580	Short	0.027994	Y	100%	WDOG_EXT_MON	SM9	80%	0.005599
					Open	0.012760						
					Value Change	0.016820						
		C32	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SM9	80%	0.005627
					Open	0.012569	Y	100%	WDOG_EXT_MON	SM9	80%	0.002514
					Value Change	0.016568	Y	100%	WDOG_EXT_MON	SM9	80%	0.003314
		C34	Y	0.2000	Short	0.097020	Y	100%	WDOG_EXT_MON	SM9	80%	0.019404
					Open	0.044000						
					Value Change	0.058000						
		C35	Y	0.2000	Short	0.097020	Y	100%	WDOG_EXT_MON	SM9	80%	0.019404
					Open	0.044000						
					Value Change	0.058000	Y	100%	WDOG_EXT_MON	SM9	80%	0.0116
		R35	Y	0.1100	Short	0.005500						
					Open	0.064251	Y	100%	WDOG_EXT_MON	SM9	80%	0.01285
					Value Change	0.039600						
	Microcontroller Programming Header	C33	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		R34	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
String		D7	Y	1.2000	Short	0.588000						

System	Sub-system	Component name	Safety Critical component	Safety Critical failure rate	Failure Mode	Multiple Point Failure rate (Perceived + latent	Failure mode that may lead to the violation of safety goal in combination with failure of another component?	Failure rate distribution, %	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode coverage with respect to Latent failures, %	Latent multiple-Point failure rate/FIT
Controller	Power Supply (PSU2)				Open	0.427680	Y	100%	WDOG_EXT_MON	SMS	80%	0.085536
					Value Change	0.180000						
		C18	Y	1.6800	Short	0.814968	Y	100%	WDOG_EXT_MON	SMS	80%	0.162994
					Open	0.365904	Y	100%	WDOG_EXT_MON	SMS	80%	0.073181
					Value Change	0.487200						
		C19	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SMS	80%	0.005627
					Open	0.012760						
					Value Change	0.016820						
		U4	Y	1.0000	All	0.495000	Y	100%	WDOG_EXT_MON	SMS	80%	0.099
					All	0.500000						
		C21	Y	1.6800	Short	0.814968	Y	100%	WDOG_EXT_MON	SMS	80%	0.162994
					Open	0.365904	Y	100%	WDOG_EXT_MON	SMS	80%	0.073181
					Value Change	0.487200						
		C20	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SMS	80%	0.005627
					Open	0.012760						
					Value Change	0.016820						
		U5	Y	0.4430	All	0.219285	Y	100%	WDOG_EXT_MON	SMS	80%	0.043857
					All	0.221500						
		C25	Y	1.6800	Short	0.814968	Y	100%	WDOG_EXT_MON	SMS	80%	0.162994
					Open	0.365904	Y	100%	WDOG_EXT_MON	SMS	80%	0.073181
					Value Change	0.487200						
		C26	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SMS	80%	0.005627
					Open	0.012760						
					Value Change	0.016820						
		C27	Y	1.6800	Short	0.814968	Y	100%	WDOG_EXT_MON	SMS	80%	0.162994
					Open	0.365904	Y	100%	WDOG_EXT_MON	SMS	80%	0.073181
					Value Change	0.487200						
		C22	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SMS	80%	0.005627
					Open	0.012760						
					Value Change	0.016820						
		U6	Y	1.0000	All	0.495000	Y	100%	WDOG_EXT_MON	SMS	80%	0.099
					All	0.500000						
		C17	Y	0.0580	Short	0.028136	Y	100%	WDOG_EXT_MON	SMS	80%	0.005627
					Open	0.012760						
					Value Change	0.016820						
		C23	Y	1.6800	Short	0.814968	Y	100%	WDOG_EXT_MON	SMS	80%	0.162994
					Open	0.365904	Y	100%	WDOG_EXT_MON	SMS	80%	0.073181
					Value Change	0.487200						
	Test Res & Driver	R87	Y	0.5000	Short	0.025000						
					Open	0.295000						
					Value Change	0.180000						
		R88	Y	0.5000	Short	0.025000						
					Open	0.295000						
					Value Change	0.180000						
		R91	Y	0.5000	Short	0.025000						
					Open	0.295000						
					Value Change	0.180000						
		Opt04	Y	1.8000	Short	0.552420						
					Open	0.450000						
					Value Change	0.306000						
					Output Low	0.392040						
					Output High	0.090000						
		Rly2	Y	10.0000	Fails Open	8.000000						
					Fails Short	1.980000						
		Q6	Y	1.2000	Short	0.605880						
					Open	0.060000						
					Value Change	0.204000						
					Output Low	0.264000						
					Output High	0.059400						
		R89	N	0.0000	Short	0.000000						
					Open	0.000000						
					Value Change	0.000000						
		LED2	N	0.0000	Fails Off	0.000000						
					Fails On	0.000000						

Table 121: BMS - Architecture 1 Actuator 1

Reference	1)A1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		0.00%	Limited	0.00%	Limited	90.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1							Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
									Low		Low		High		Low		High		High		
									60%		60%		99%		60%		99%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low	Medium	High																	
		60%	90%	99%																	
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	20%	0%	0%	y	➤												
		Welded Contacts	Welded Contacts	Welded Contacts	5%	0%	0%	y	➤												
			Individual welded contacts	Individual welded contacts	10%	0%	0%	y	➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	y			➤		➤	y							PCc_PSU_Mon
			Drift	Drift & Oscillation	15%	0%	0%	y			➤		➤	y							PCc_PSU_Mon
				Power Spikes	5%	0%	0%	y			➤		➤	y							PCc_PSU_Mon
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	10%	0%	0%								➤		➤		➤		
				Incorrect action	15%	0%	0%	y							➤		➤		➤		
				Delayed Action	10%	0%	0%	y							➤		➤		➤		
									0.00%		0.00%		29.70%		0%		0%		0%		

BMS - Architecture 1 Actuator 2

Similar techniques as Architecture 1 Actuator 1 so not shown.

Table 122: BMS - Architecture 1 Connection 1

Reference	1)C1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description Technique from ISO26262		Specific PCC
Table 26262-5: 2011		100%			42.00%	Limited	42.00%	Limited	100.00%	Failure Detection by on-line monitoring		
		Maintain Cells in Operating Area Architecture Candidate 1								High		
										99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low	Medium	High								
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	12%	12%	y		➤	y	PCc_6803_Self_Test
				Contact resistance	10%	0%	0%	y		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	18%	18%	y		➤	y	PCc_6803_Self_Test
			Short Circuit to Vbat	Short Circuit to Vbat	20%	12%	12%	y		➤	Y	PCc_6803_Self_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y		➤		
				Resistive drift between pins / signal lines	10%	0%	0%	y		➤		
										69.30%		

Table 123: BMS - Architecture 1 Connection 2

Reference	1)C2	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			72.00%	Low	72.00%	Low	100.00%	Technique from ISO26262		
		Maintain Cells in Operating Area Architecture Candidate 1								Failure Detection by on-line monitoring High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	18%	18%	y		➤	y	PCc_6803_Self_Test
				Contact resistance	10%	0%	0%	y		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	27%	27%	y		➤	y	PCc_6803_Self_Test
			Short Circuit to Vbat	Short Circuit to Vbat	20%	18%	18%	y		➤	y	PCc_6803_Self_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	9%	9%	y		➤	y	PCc_6803_Self_Test
				Resistive drift between pins / signal lines	10%	0%	0%	y		➤		
										79.20%		

Table 124: BMS - Architecture 1 Connection 3

Reference	1)C3	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	70.00%	Technique from ISO26262		
		Maintain Cells in Operating Area Architecture Candidate 1								Failure Detection by on-line monitoring High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	0%	0%	y		➤		
				Contact resistance	10%	0%	0%	y		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	0%	0%	y		➤		
			Short Circuit to Vbat	Short Circuit to Vbat	20%	0%	0%			➤		
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%			➤		
				Resistive drift between pins / signal lines	10%	0%	0%	y		➤		
										49.50%		

BMS - Architecture 1 Connection 4

Similar techniques as Architecture 1 Connection 3 so not shown.

Table 125: BMS - Architecture 1 Data 1 (subset 1)

Reference	1)D1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description							
		100%			93.60%	Medium	90.79%	Medium	100.00%	Technique from ISO26262							
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1								Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Specific PCC
										High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution		Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	
		Low 60%	Medium 90%	High 99%																		
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range			0%	0%														
			Offsets	Offsets			0%	0%														
		Stuck in range	Stuck in range	Stuck in range			0%	0%														
				Oscillation			0%	0%														
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	25%		25%	24%	y													PCc_Data_Checksum, PCc_Poll_Response_Time
		Message corruption	Message corruption	Message corruption	15%		15%	14%	y													PCc_Data_Checksum, PCc_Poll_Response_Time
		Message Delay	Message Delay	Message Delay	20%		18%	17%	y													PCc_Poll_Response_Time
		Message Loss	Message Loss	Message Loss	15%		14%	13%	y													PCc_Poll_Response_Time
		Unintended message repetition	Unintended message repetition	Unintended message repetition	10%		9%	9%	y													PCc_Poll_Response_Time
			Resequencing	Resequencing	5%		5%	4%	y													PCc_Poll_Response_Time
			Insertion of message	Insertion of message	5%		5%	4%	y													PCc_Poll_Response_Time
				Masquerading	5%		5%	4%	y													PCc_Poll_Response_Time
										0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		

Table 126: BMS - Architecture 1 Data 1 (subset 2)

Reference	1)D1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														
		100%			93.60%	Medium	90.79%	Medium	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1								One-bit hardware redundancy		Multi-bit hardware redundancy		Read back of sent message		Complete hardware redundancy		Inspection using test patterns		Transmission redundancy		Information redundancy		PCc_Frame_Seq		Timeout monitoring		Combination of information, Redundancy, frame count, and timeout		Specific PCC
										Low 60%		Medium 90%		Medium 90%		High 99%		High 99%		Medium 90%		Medium 90%		Medium 90%		Medium 90%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution		Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.7.1	Used	D.2.7.2	Used	D.2.7.9	Used	D.2.7.3	Used	D.2.7.4	Used	D.2.7.5	Used	D.2.7.6	Used	D.2.7.7	Used	D.2.7.8	Used	D.2.7.6,7,8	Used	
		Low 60%	Medium 90%	High 99%																										
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range			0%	0%																						
			Offsets	Offsets			0%	0%																						
		Stuck in range	Stuck in range	Stuck in range			0%	0%																						
				Oscillation			0%	0%																						
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	25%		25%	24%	y																			y		PCc_Data_Checksum, PCc_Poll_Response_Time
		Message corruption	Message corruption	Message corruption	15%		15%	14%	y																			y		PCc_Data_Checksum, PCc_Poll_Response_Time
		Message Delay	Message Delay	Message Delay	20%		18%	17%	y																	y				PCc_Poll_Response_Time
		Message Loss	Message Loss	Message Loss	15%		14%	13%	y																	y				PCc_Poll_Response_Time
		Unintended message repetition	Unintended message repetition	Unintended message repetition	10%		9%	9%	y																	y				PCc_Poll_Response_Time
			Resequencing	Resequencing	5%		5%	4%	y																	y				PCc_Poll_Response_Time
			Insertion of message	Insertion of message	5%		5%	4%	y																	y				PCc_Poll_Response_Time
				Masquerading	5%		5%	4%	y																	y				PCc_Poll_Response_Time
										0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		54.00%		39.60%		

BMS - Architecture 1 Data 2

Similar techniques as Architecture 1 Data 1 so not shown.

BMS - Architecture 1 Data 3

Similar techniques as Architecture 1 Data 1 so not shown.

BMS - Architecture 1 Data 5

Similar techniques as Architecture 1 Data 1 so not shown.

Table 127: BMS - Architecture 1 Measurement 1

Reference	1)M1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%		60.00%	Low	58.80%	Limited	85.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1							Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data	
									High	Low	High	Medium	High	High	High		
									99%	60%	99%	90%	99%	99%	99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	D.2.1.1	D.2.6.1	D.2.6.2	D.2.6.3	D.2.6.4	D.2.6.5		
		Low	Medium	High					Used	Used	Used	Used	Used	Used	Used		
		60%	90%	99%													
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	0%	0%										
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	6%	6%	Y		Y							PCc_OA_Window, PCc_6803_Self_Test
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	9%	9%	Y		Y							PCc_OA_Window, PCc_6803_Self_Test
			Short Circuit to Vbat	Short Circuit to Vbat	10%	6%	6%	y		Y							PCc_OA_Window, PCc_6803_Self_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	6%	6%	y		Y							PCc_6803_Self_Test
			Offsets	Offsets	15%	9%	9%	y		Y							PCc_6803_Self_Test
		Stuck in range	Stuck in range	Stuck in range	15%	9%	9%	y		Y							PCc_6803_Self_Test
			Drift & Oscillation	Drift & Oscillation	10%	6%	6%	y		Y							PCc_6803_Self_Test
									0.00%	51.00%	0.00%	0.00%	0.00%	0.00%	0.00%		

Table 128: BMS - Architecture 1 Measurement 2

Reference	1)M2	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1							Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within	
									High	Low	High	Medium	High	High	High		
									99%	60%	99%	90%	99%	99%	99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	D.2.1.1	D.2.6.1	D.2.6.2	D.2.6.3	D.2.6.4	D.2.6.5		
		Low	Medium	High					Used	Used	Used	Used	Used	Used	Used		
		60%	90%	99%													
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	0%	0%	y									
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	6%	6%	y									
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	9%	9%	y									
			Short Circuit to Vbat	Short Circuit to Vbat	10%	6%	6%	y									
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	6%	6%	y									
			Offsets	Offsets	15%	0%	0%	y									
		Stuck in range	Stuck in range	Stuck in range	15%	9%	9%	y									
			Drift & Oscillation	Drift & Oscillation	10%	0%	0%	y									
									0.00%	30.00%	9.90%	0.00%	0.00%	0.00%	0.00%		

BMS - Architecture 1 Measurement 6

Similar techniques as Architecture 1 Measurement 2 so not shown.

Table 129: BMS - Architecture 1 Output 1

Reference	1)O1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	60.00%	Technique from ISO26262												
		Maintain Cells in Operating Area Architecture Candidate 1								Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better		Voltage or current control (input)		Voltage or current control (output)		
										Low		High		Medium		High		High		High		Low		High		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim		Failure Mode Leads to Violation of Safety Goal	60%		99%		90%		99%		99%		99%		60%		99%		
		Low	Medium	High						D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		60%	90%	99%																						
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	15%	0%	0%			➤		➤		➤		➤		➤		➤						
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%			➤		➤		➤		➤		➤		➤						
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	Y		➤		➤		➤		➤		➤		➤						
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y		➤		➤		➤		➤		➤		➤						
			Offsets	Offsets	5%	0%	0%			➤		➤		➤		➤		➤		➤						
		Stuck in range	Stuck in range	Stuck in range	10%	0%	0%	Y		➤		➤		➤		➤		➤		➤						
				Drift & Oscillation	5%	0%	0%			➤		➤		➤		➤		➤		➤						
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	5%	0%	0%	y														➤		➤	y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	0%	0%	y														➤		➤	y	PCc_PSU_Mon
				Power Spikes	5%	0%	0%	y														➤		➤	y	PCc_PSU_Mon
										0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		29.70%		

Table 130: BMS - Architecture 1 Output 2

Reference	1)O2	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	60.00%	Technique from ISO26262												
		Maintain Cells in Operating Area Architecture Candidate 1								Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better		Voltage or current control (input)		Voltage or current control (output)		
										Low		High		Medium		High		High		High		Low		High		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim		Failure Mode Leads to Violation of Safety Goal	60%		99%		90%		99%		99%		99%		60%		99%		
		Low	Medium	High						D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		60%	90%	99%																						
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	15%	0%	0%			➤		➤		➤		➤		➤		➤						
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%			➤		➤		➤		➤		➤		➤						
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	Y		➤		➤		➤		➤		➤		➤						
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y		➤		➤		➤		➤		➤		➤						
			Offsets	Offsets	5%	0%	0%			➤		➤		➤		➤		➤		➤						
		Stuck in range	Stuck in range	Stuck in range	10%	0%	0%	Y		➤		➤		➤		➤		➤		➤						
				Drift & Oscillation	5%	0%	0%			➤		➤		➤		➤		➤		➤						
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	5%	0%	0%	y														➤		➤	y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	0%	0%	y														➤		➤	y	PCc_PSU_Mon
				Power Spikes	5%	0%	0%	y														➤		➤	y	PCc_PSU_Mon
										0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		29.70%		

Table 131: BMS - Architecture 1 Parameter 1 (subset 1)

Reference	1)P1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
Table 26262-5: 2011		100%			95.50%	Medium	94.08%	Medium	90.00%	Technique from ISO26262										
		Maintain Cells in Operating Area Architecture Candidate 1								Voltage or current control (input)		Voltage or current control (output)		Watchdog with separate time base without time-window		Watchdog with separate time base and time-window		Logical monitoring of program sequence		Combination of temporal and logical monitoring of program sequences		Combination of temporal and logical monitoring of program sequences with time dependency		
										Low		High		Low		Medium		Medium		High		High		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim		Failure Mode Leads to Violation of Safety Goal	60%		99%		60%		90%		90%		99%		99%		
		Low	Medium	High						D.2.8.1	Used	D.2.8.2	Used	D.2.9.1	Used	D.2.9.2	Used	D.2.9.3	Used	D.2.9.4	Used	D.2.9.5	Used	
		60%	90%	99%																				
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y		➤		➤	y											PCc_PSU_Mon
			Drift	Drift & Oscillation	10%	10%	10%	y		➤		➤	y											PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y		➤		➤	y											PCc_PSU_Mon
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	4%	y						➤		➤		➤	y	➤		➤		PCc_Code_Seq
			dc fault model	dc fault model	5%	5%	4%	y						➤		➤		➤	y	➤		➤		PCc_Code_Seq
				Incorrect frequency	10%	9%	9%	y						➤		➤		➤	y	➤		➤		PCc_Code_Seq
				Period jitter	10%	9%	9%	y						➤		➤		➤	y	➤		➤		PCc_Code_Seq
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%																	
			dc fault model	dc fault model	5%	0%	0%																	
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y																PCc_RAM_Test
			dc fault model	dc fault model	5%	5%	5%	y																PCc_RAM_Test
				soft error model	5%	5%	5%	y																PCc_RAM_Test
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y																PCc_Micro_Test
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y																PCc_Micro_Test
				dc fault model	5%	5%	5%	y																PCc_Micro_Test
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y																PCc_Micro_Test
										0.00%		24.75%		0.00%		0.00%		27.00%		0.00%		0.00%		

Table 132: BMS - Architecture 1 Parameter 1 (subset 2)

Reference	1)P1	Failure Mode Distribution			Full Claim		PCc Claim	SG Failure Distribution
		100%			95.50%	Medium	94.08% Medium	90.00%
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1						
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage: Low 60%	Medium 90%	High 99%	Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y
			Drift	Drift & Oscillation	10%	10%	10%	y
				Power Spikes	5%	5%	5%	y
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	4%	y
			dc fault model	dc fault model	5%	5%	4%	y
				Incorrect frequency	10%	9%	9%	y
				Period jitter	10%	9%	9%	y
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%	
			dc fault model	dc fault model	5%	0%	0%	
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y
			dc fault model	dc fault model	5%	5%	5%	y
			soft error model	soft error model	5%	5%	5%	y
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y
				dc fault model	5%	5%	5%	y
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y

Technique Description – Technique from ISO26262

Element	Parity bit (Low 60%) D.2.5.2 Used	Memory monitoring using error-detection-correction codes (EDC) (High 99%) D.2.4.1 Used	Modified checksum (Low 60%) D.2.4.2 Used	Memory signature (High 99%) D.2.4.3 Used	Block replication (for example double memory with hardware or software comparison) (High 99%) D.2.4.4 Used	RAM Pattern test (Medium 90%) D.2.5.1 Used	RAM March test (High 99%) D.2.5.3 Used	Parity bit (Low 60%) D.2.5.2 Used	Memory monitoring using error-detection-correction codes (EDC) (High 99%) D.2.4.1 Used	Block replication (for example double memory with hardware or software comparison) (High 99%) D.2.4.4 Used	Running checksum/CRC (High 99%) D.2.5.4 Used	Specific PCC
Power supply												PCc_PSU_Mon
												PCc_PSU_Mon
												PCc_PSU_Mon
Clock												PCc_Code_Seq
												PCc_Code_Seq
												PCc_Code_Seq
												PCc_Code_Seq
Non-volatile Memory												
Volatile Memory						y					y	PCc_RAM_Test
						y					y	PCc_RAM_Test
						y					y	PCc_RAM_Test
Processing Units : ALU - Data Path (D.4)												PCc_Micro_Test
												PCc_Micro_Test
												PCc_Micro_Test
Processing Units : ALU - Data Path (D.13)												PCc_Micro_Test
	0.00%	0.00%	0.00%	0.00%	0.00%	13.50%	0.00%	0.00%	0.00%	0.00%	14.85%	

Table 133: BMS - Architecture 1 Parameter 1 (subset 3)

Reference	1)P1	Failure Mode Distribution			Full Claim		PCc Claim	SG Failure Distribution
		100%			95.50%	Medium	94.08% Medium	90.00%
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1						
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage: Low 60%	Medium 90%	High 99%	Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y
			Drift	Drift & Oscillation	10%	10%	10%	y
				Power Spikes	5%	5%	5%	y
Clock	D.10	stuck at	stuck at	stuck at	5%	5%	4%	y
			dc fault model	dc fault model	5%	5%	4%	y
				Incorrect frequency	10%	9%	9%	y
				Period jitter	10%	9%	9%	y
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	5%	0%	0%	
			dc fault model	dc fault model	5%	0%	0%	
Volatile Memory	D.6	stuck at	stuck at	stuck at	5%	5%	5%	y
			dc fault model	dc fault model	5%	5%	5%	y
			soft error model	soft error model	5%	5%	5%	y
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	5%	5%	5%	y
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	y
				dc fault model	5%	5%	5%	y
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	y

Technique Description – Technique from ISO26262

Element	Self-test by software (Medium 90%) D.2.3.1 Used	Self-test by software cross exchanged between two independent units (Medium 90%) D.2.3.3 Used	Self-test supported by hardware (one-channel) (Medium 90%) D.2.3.2 Used	Software diversified redundancy (one hardware channel) (High 99%) D.2.3.4 Used	Reciprocal comparison by software in separate processing units (High 99%) D.2.3.5 Used	HW redundancy (e.g. Dual Core Lockstep, asymmetric redundancy, coded processing) (High 99%) D.2.3.6 Used	Configuration register test (High 99%) D.2.3.7 Used	Stack over/under flow detection (Low 60%) D.2.3.8 Used	Integrated hardware consistency monitoring (High 99%) D.2.3.9 Used	Self-test by software (Medium 90%) D.2.3.1 Used	Self-test supported by hardware (one-channel) (High 99%) D.2.3.2 Used	Specific PCC
Power supply												PCc_PSU_Mon
												PCc_PSU_Mon
												PCc_PSU_Mon
Clock												PCc_Code_Seq
												PCc_Code_Seq
												PCc_Code_Seq
												PCc_Code_Seq
Non-volatile Memory												
Volatile Memory												PCc_RAM_Test
												PCc_RAM_Test
												PCc_RAM_Test
Processing Units : ALU - Data Path (D.4)							y					PCc_Micro_Test
							y					PCc_Micro_Test
							y					PCc_Micro_Test
Processing Units : ALU - Data Path (D.13)										y		PCc_Micro_Test
	0%	0%	0%	0%	0%	0%	15%	0%	0%	5%	0%	

BMS - Architecture 1 Parameter 2

Similar techniques as Architecture 1 Parameter 1 so not shown.

BMS - Architecture 1 Parameter 4

Similar techniques as Architecture 1 Parameter 1 so not shown.

BMS - Architecture 1 Parameter 5

Similar techniques as Architecture 1 Parameter 1 so not shown.

BMS - Architecture 1 Parameter 8

Similar techniques as Architecture 1 Parameter 1 so not shown.

BMS - Architecture 1 Parameter 14

Similar techniques as Architecture 1 Parameter 1 so not shown.

Table 134: BMS - Architecture 1 Power Supply Unit 1

Reference	1)PSU1	Failure Mode Distribution			Full Claim	PCc Claim	Technique Description				Specific PCC
		100%			99%	99%	Technique from ISO26262				
Table D.9 26262-5: 2011							Voltage or current control (input)		Voltage or current control (output)		
							Low 60%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%								
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	50%	50%	49%	➤		➤	y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	➤		➤	y	PCc_PSU_Mon
				Power Spikes	30%	30%	30%	➤		➤	y	PCc_PSU_Mon
								0.00%		99.00%		

BMS - Architecture 1 PSU 2

Similar techniques as Architecture 1 PSU 1 so not shown.

BMS - Architecture 1 PSU 3

Similar techniques as Architecture 1 PSU 1 so not shown.

Table 135: BMS - Architecture 1 Transducer 1

Reference	1)T1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			99.00%	High	97.74%	Medium	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1								Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Voltage or current control (input)		Voltage or current control (output)		
										High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		Low 60%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim		Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																						
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	20%	20%		y	➤	y	➤		➤		➤	y			➤						PCc_OA_Window, PCc_6803_Self_Test
			Offsets	Offsets	10%	10%	10%		y	➤	y	➤		➤		➤		➤		➤						PCc_6803_Self_Test
		Stuck in range	Stuck in range	Stuck in range	30%	30%	29%		y	➤	y	➤		➤		➤		➤		➤						PCc_6803_Self_Test
				Oscillation	5%	5%	5%		y	➤	y	➤		➤		➤		➤		➤						PCc_6803_Self_Test
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%		y													➤		➤	y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%		y													➤		➤	y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%		y													➤		➤	y	PCc_PSU_Mon
										64.35%		0.00%		0.00%		12.00%		0.00%		0.00%		0.00%		34.65%		

Appendix E2 – BMS – Architecture 2 DC% Claims

Table 136: BMS - Architecture 2 Actuator 3

Reference	2)A3	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		99.00%	High	98.28%	Medium	55.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 2							Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
									Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low	Medium	High																	
		60%	90%	99%																	
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	20%	0%	0%		➤												
		Welded Contacts	Welded Contacts	Welded Contacts	5%	0%	0%		➤												
			Individual welded contacts	Individual welded contacts	10%	0%	0%		➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y			➤		➤	y							PCc_PSU_Mon
			Drift	Drift & Oscillation	15%	15%	15%	y			➤		➤	y							PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y			➤		➤	y							PCc_PSU_Mon
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	10%	0%	0%								➤		➤		➤		
				Incorrect action	15%	15%	15%	y							➤		➤		➤	y	PCc_5kHzSelf_Test
				Delayed Action	10%	10%	10%	y							➤		➤		➤	y	PCc_5kHzSelf_Test
									0.00%		0.00%		29.70%		0%		0%		25%		

Table 137: BMS - Architecture 2 Actuator 4

Reference	2)A4	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%			0.00%	Limited	0.00%	Limited	90.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 2								Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
										Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low	Medium	High																	
		60%	90%	99%																	
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	20%	0%	0%	y	➤												
		Welded Contacts	Welded Contacts	Welded Contacts	5%	0%	0%	y	➤												
			Individual welded contacts	Individual welded contacts	10%	0%	0%	y	➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	y			➤		➤	y							PCc_PSU_Mon
			Drift	Drift & Oscillation	15%	0%	0%	y			➤		➤	y							PCc_PSU_Mon
				Power Spikes	5%	0%	0%	y			➤		➤	y							PCc_PSU_Mon
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	10%	0%	0%								➤		➤		➤		
				Incorrect action	15%	0%	0%	y							➤		➤		➤		
				Delayed Action	10%	0%	0%	y							➤		➤		➤		
									0.00%		0.00%		29.70%		0%		0%		0%		

BMS - Architecture 2 Actuator 6

Similar techniques as Architecture 2 Actuator 4 so not shown.

BMS - Architecture 2 Actuator 7

Similar techniques as Architecture 2 Actuator 4 so not shown.

Table 138: BMS - Architecture 2 Connection 1

Reference	2)C1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description Technique from ISO26262		Specific PCC
Table 26262-5: 2011		100%			72.00%	Low	72.00%	Low	100.00%	Failure Detection by on-line monitoring		
		Maintain Cells in Operating Area Architecture Candidate 2								High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	18%	18%	y		➤	y	PCc6801_Self_Test
				Contact resistance	10%	0%	0%	y		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	27%	27%	y		➤	y	PCc6801_Self_Test
			Short Circuit to Vbat	Short Circuit to Vbat	20%	18%	18%	y		➤	Y	PCc6801_Self_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	9%	9%	y		➤	Y	PCc6801_Self_Test
				Resistive drift between pins / signal lines	10%	0%	0%	y		➤		
										79.20%		

BMS - Architecture 2 Connection 2

Similar techniques as Architecture 2 Connection 1 so not shown.

Table 139: BMS - Architecture 2 Connection 5

Reference	2)C5	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description Technique from ISO26262		Specific PCC
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	100.00%	Failure Detection by on-line monitoring		
		Maintain Cells in Operating Area Architecture Candidate 2								High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	0%	0%	y		➤		
				Contact resistance	10%	0%	0%	y		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	0%	0%	y		➤		
			Short Circuit to Vbat	Short Circuit to Vbat	20%	0%	0%	y		➤		
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y		➤		
				Resistive drift between pins / signal lines	10%	0%	0%	y		➤		
										0.00%		

BMS - Architecture 2 Connection 6

Similar techniques as Architecture 2 Connection 5 so not shown.

Table 140: BMS - Architecture 2 Measurement 1

Reference	2)M1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%			99.00%	High	98.21%	Medium	85.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 2								Failure Detection by on-line monitoring		Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		
										High 99%		Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	
		Low	Medium	High																				
		60%	90%	99%																				
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	0%	0%			➤														
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	10%	10%	y				➤	y	➤	y	➤		➤		➤		➤	Y	PCc_OA_Window, PCc_6803_Self_Test
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	15%	15%	y				➤	y	➤	y	➤		➤		➤		➤	Y	PCc_OA_Window, PCc_6803_Self_Test
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	y				➤	y	➤	y	➤		➤		➤		➤	Y	PCc_OA_Window, PCc_6803_Self_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y				➤		➤	y	➤		➤		➤		➤	Y	PCc_6803_Self_Test
			Offsets	Offsets	15%	15%	15%	y				➤		➤	Y	➤		➤		➤		➤	Y	PCc_6803_Self_Test
		Stuck in range	Stuck in range	Stuck in range	15%	15%	15%	y				➤		➤	y	➤		➤		➤		➤	Y	PCc_6803_Self_Test
			Drift & Oscillation	Drift & Oscillation	10%	10%	10%	y				➤		➤	Y	➤		➤		➤		➤	Y	PCc_6803_Self_Test
										0.00%		21.00%		84.15%		0.00%		0.00%		0.00%		84.15%		

Table 141: BMS - Architecture 2 Measurement 3

Reference	2)M3	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			65.85%	Low	64.83%	Low	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 2								Failure Detection by on-line monitoring		Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		
										High 99%		Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	
		Low	Medium	High																				
		60%	90%	99%																				
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	15%	15%	Y		➤	Y													
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	6%	6%	Y				➤	Y	➤		➤		➤		➤		➤		PCc_HW_MONITOR
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	9%	9%	Y				➤	Y	➤		➤		➤		➤		➤		PCc_HW_MONITOR
			Short Circuit to Vbat	Short Circuit to Vbat	10%	6%	6%	Y				➤	Y	➤		➤		➤		➤		➤		PCc_HW_MONITOR
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	6%	6%	Y				➤	Y	➤		➤		➤		➤		➤		PCc_HW_MONITOR
			Offsets	Offsets	15%	9%	9%	Y				➤	Y	➤		➤		➤		➤		➤		PCc_HW_MONITOR
		Stuck in range	Stuck in range	Stuck in range	15%	9%	9%	Y				➤	Y	➤		➤		➤		➤		➤		PCc_HW_MONITOR
			Drift & Oscillation	Drift & Oscillation	10%	6%	6%	Y				➤	Y	➤		➤		➤		➤		➤		PCc_HW_MONITOR
										14.85%		51.00%		0.00%		0.00%		0.00%		0.00%		0.00%		

Table 142: BMS - Architecture 2 Measurement 4

Reference	2)M4	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description							
		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262							
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 2								Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Specific PCC
										High	Low	High	Medium	High	High	High	
										99%	60%	99%	90%	99%	99%	99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	D.2.1.1	D.2.6.1	D.2.6.2	D.2.6.3	D.2.6.4	D.2.6.5	
		Low	Medium	High						Used	Used	Used	Used	Used	Used	Used	
		60%	90%	99%													
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	0%	0%	y									
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	0%	0%	y									
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%	y									
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	y									
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y									
			Offsets	Offsets	15%	0%	0%	y									
		Stuck in range	Stuck in range	Stuck in range	15%	0%	0%	y									
			Drift & Oscillation	Drift & Oscillation	10%	0%	0%	y									
										0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	

BMS - Architecture 2 Measurement 5

Similar techniques as Architecture 2 Measurement 4 so not shown.

Table 143: BMS - Architecture 2 Output 3

Reference	2)O3	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description													
		100%			60.00%	Low	59.16%	Limited	100.00%	Technique from ISO26262													
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 2								Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		Specific PCC
										Low		High		Medium		High		High		High		Low		High		
										60%		99%		90%		99%		99%		99%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																						
		60%	90%	99%																						
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit		0%	0%																			
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)		0%	0%																			
			Short Circuit to Vbat	Short Circuit to Vbat	30%	18%	18%	y			y															PCC_OA_TRIP
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	6%	6%	y			y															PCC_OA_TRIP
			Offsets	Offsets		0%	0%																			
		Stuck in range	Stuck in range	Stuck in range	20%	12%	12%	Y			y															PCC_OA_TRIP
				Drift & Oscillation		0%	0%																			
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	30%	18%	18%	y															y			PCc_PSU_Mon
			Drift	Drift & Oscillation	5%	3%	3%	y															y			PCc_PSU_Mon
				Power Spikes	5%	3%	3%	y															y			PCc_PSU_Mon
										36.00%		0.00%		0.00%		0.00%		0.00%		0.00%		24.00%		0.00%		

Table 144: BMS - Architecture 2 Output 5

Reference	2)O5	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		0.00%	Limited	0.00%	Limited	60.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 2							Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		
									Low		High		Medium		High		High		High		Low		High		
									60%		99%		90%		99%		99%		99%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																					
		60%	90%	99%																					
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	15%	0%	0%																		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%																		
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	y																	
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	y																	
			Offsets	Offsets	5%	0%	0%																		
		Stuck in range	Stuck in range	Stuck in range	10%	0%	0%	Y																	
				Drift & Oscillation	5%	0%	0%																		
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	5%	0%	0%	y																y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	0%	0%	y																y	PCc_PSU_Mon
				Power Spikes	5%	0%	0%	y																y	PCc_PSU_Mon
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		29.70%		

BMS - Architecture 2 output 6

Similar techniques as Architecture 2 output 5 so not shown.

Table 145: BMS - Architecture 2 Transducer 3

Reference	2)T3	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%		73.65%	Low	72.70%	Low	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 2							Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid. range		Sensor Correlation		Sensor rationality Check		Voltage or current control (input)		Voltage or current control (output)		
									High		High		High		Low		High		Medium		Low		High		
									99%		99%		99%		60%		99%		99%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																					
		60%	90%	99%																					
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	12%	12%	y								y									PCc6801_Self_Test
			Offsets	Offsets	10%	6%	6%	y								y									PCc6801_Self_Test
		Stuck in range	Stuck in range	Stuck in range	30%	18%	18%	y								y									PCc6801_Self_Test
				Oscillation	5%	3%	3%	y								y									PCc6801_Self_Test
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y																y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	y																y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y																y	PCc_PSU_Mon
									0.00%		0.00%		0.00%		39.00%		0.00%		0.00%		0.00%		34.65%		

Table 146: BMS - Architecture 2 Transducer 4

Reference	2)T4	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 2							Failure Detection by on-line monitoring	Test Pattern	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Sensor valid range	Sensor Correlation	Sensor rationality Check	Voltage or current control (input)	Voltage or current control (output)	
									High 99%	High 99%	High 99%	Low 60%	High 99%	Medium 90%	Low 60%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1 Used	D.2.6.1 Used	D.2.6.5 Used	D.2.10.1 Used	D.2.10.2 Used	D.2.10.3 Used	D.2.8.1 Used	D.2.8.2 Used	
		Low 60%	Medium 90%	High 99%													
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	0%	0%	y									
			Offsets	Offsets	10%	0%	0%	y									
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y									
				Oscillation	5%	0%	0%	y									
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	y								y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	0%	0%	y								y	PCc_PSU_Mon
				Power Spikes	5%	0%	0%	y								y	PCc_PSU_Mon
									0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	34.65%	

Appendix E3 – BMS – Architecture 3 DC% Claims

Table 147: BMS - Architecture 3 Transducer 3

Reference	3)T3	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%		73.65%	Low	72.70%	Low	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 3							Failure Detection by on-line monitoring	Test Pattern	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Sensor valid range	Sensor Correlation	Sensor rationality Check	Voltage or current control (input)	Voltage or current control (output)	
									High 99%	High 99%	High 99%	Low 60%	High 99%	Medium 90%	Low 60%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1 Used	D.2.6.1 Used	D.2.6.5 Used	D.2.10.1 Used	D.2.10.2 Used	D.2.10.3 Used	D.2.8.1 Used	D.2.8.2 Used	
		Low 60%	Medium 90%	High 99%													
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	12%	12%	y				Y					PCc6801_Self_Test
			Offsets	Offsets	10%	6%	6%	y				Y					PCc6801_Self_Test
		Stuck in range	Stuck in range	Stuck in range	30%	18%	18%	y				Y					PCc6801_Self_Test
				Oscillation	5%	3%	3%	y				Y					PCc6801_Self_Test
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y								Y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	y								Y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y								Y	PCc_PSU_Mon
									0.00%	0.00%	0.00%	39.00%	0.00%	0.00%	0.00%	34.65%	

Appendix E4 – BMS – Architecture 4 DC% Claims

Table 148: BMS - Architecture 4 Actuator 5

Reference	4)A5	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%			64.29%	Low	64.29%	Low	35.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 4								Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
										Low		Low		High		Low		High		High		
										60%		60%		99%		60%		99%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low	Medium	High																		
		60%	90%	99%																		
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	20%	0%	0%			➤												
		Welded Contacts	Welded Contacts	Welded Contacts	5%	0%	0%			➤												
			Individual welded contacts	Individual welded contacts	10%	0%	0%			➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%					➤		➤								
			Drift	Drift & Oscillation	15%	0%	0%					➤		➤								
				Power Spikes	5%	0%	0%					➤		➤								
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	10%	9%	9%	y								➤	y	➤	y	➤	y	PCc_5kHzSelft_Test
				Incorrect action	15%	14%	14%	y								➤	y	➤	y	➤	y	PCc_5kHzSelft_Test
				Delayed Action	10%	0%	0%	y								➤		➤		➤		
										0.00%		0.00%		0.00%		15%		25%		25%		

Table 149: BMS - Architecture 4 Data 11 (subset 1)

Reference	1)D11	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			99.00%	High	96.03%	Medium	26.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1								Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes		Sensor valid range		Sensor Correlation		Sensor rationality Check		
										High		High		High		Low		High		Medium		
										99%		99%		99%		60%		99%		90%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	
		Low	Medium	High																		
		60%	90%	99%																		
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%			➤		➤		➤		➤				➤		
			Offsets	Offsets	10%	0%	0%			➤		➤		➤				➤		➤		
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%			➤		➤		➤				➤		➤		
				Oscillation	4%	0%	0%			➤		➤		➤				➤		➤		
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	15%	14%	Y														PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time
		Message corruption	Message corruption	Message corruption	2%	2%	2%	Y														PCc_Data_Checksum
		Message Delay	Message Delay	Message Delay	3%	3%	3%	Y														PCc_Poll_Response_Time
		Message Loss	Message Loss	Message Loss	2%	2%	2%	Y														PCc_Frame_Seq
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	1%	1%	Y														PCc_Frame_Seq
			Resequencing	Resequencing	1%	1%	1%	Y														PCc_Frame_Seq
			Insertion of message	Insertion of message	1%	1%	1%	Y														PCc_Frame_Seq
				Masquerading	1%	1%	1%	Y														PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time.
										0.00%		0.00%		73.26%		0.00%		0.00%		0.00%		

Table 150: BMS - Architecture 4 Data 11 (subset 2)

Reference	1)D11	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description / Technique from ISO26262																				Specific PCC
		100%		99.00%	High	96.03%	Medium	26.00%																					
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1							One-bit hardware redundancy		Multi-bit hardware redundancy		Read back of sent message		Complete hardware redundancy		Inspection using test patterns		Transmission redundancy		Information redundancy		PCc_Frame_Seq		Timeout monitoring		Combination of information Redundancy,frame count and timeout		
									Low 60%		Medium 90%		Medium 90%		High 99%		High 99%		Medium 90%		Medium 90%		Medium 90%		Medium 90%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.7.1	Used	D.2.7.2	Used	D.2.7.9	Used	D.2.7.3	Used	D.2.7.4	Used	D.2.7.5	Used	D.2.7.6	Used	D.2.7.7	Used	D.2.7.8	Used	D.2.7.6,7,8	Used	
		Low	Medium	High																									
		60%	90%	99%																									
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%																						
			Offsets	Offsets	10%	0%	0%																						
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%																						
				Oscillation	4%	0%	0%																						
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	15%	14%	Y	➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time
		Message corruption	Message corruption	Message corruption	2%	2%	2%	Y	➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Data_Checksum
		Message Delay	Message Delay	Message Delay	3%	3%	3%	Y	➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Poll_Response_Time
		Message Loss	Message Loss	Message Loss	2%	2%	2%	Y	➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Frame_Seq
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	1%	1%	Y	➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Frame_Seq
			Resequencing	Resequencing	1%	1%	1%	Y	➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Frame_Seq
			Insertion of message	Insertion of message	1%	1%	1%	Y	➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Frame_Seq
				Masquerading	1%	1%	1%	Y	➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time.
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		25.74%		

Table 151: BMS - Architecture 4 Measurement 4

Reference	4)M4	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description / Technique from ISO26262														Specific PCC
		100%		45.00%	Limited	44.64%	Limited	100.00%															
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 4							Failure Detection by on-line monitoring		Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		
									High 99%		Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	
		Low	Medium	High																			
		60%	90%	99%																			
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	9%	9%	y	➤	y													PCc_5kHzSelft_Test
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	6%	6%	y			➤	y	➤	y	➤		➤		➤		➤		PCc_5kHzSelft_Test
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	9%	9%	y			➤	y	➤	y	➤		➤		➤		➤		PCc_5kHzSelft_Test
			Short Circuit to Vbat	Short Circuit to Vbat	10%	6%	6%	y			➤	y	➤	y	➤		➤		➤		➤		PCc_5kHzSelft_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	6%	6%	y			➤	y	➤	y	➤		➤		➤		➤		PCc_5kHzSelft_Test
			Offsets	Offsets	15%	0%	0%	y			➤		➤		➤		➤		➤		➤		
		Stuck in range	Stuck in range	Stuck in range	15%	9%	9%	y			➤	y	➤	y	➤		➤		➤		➤		PCc_5kHzSelft_Test
			Drift & Oscillation	Drift & Oscillation	10%	0%	0%	y			➤		➤		➤		➤		➤		➤		
									14.85%		36.00%		59.40%		0.00%		0.00%		0.00%		0.00%		

Table 152: BMS - Architecture 4 Output 7

Reference	4)O7	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description / Technique from ISO26262																Specific PCC
		100%		99.00%	High	97.52%	Medium	90.00%																	
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 4							Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		
									Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		Low 60%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																					
		60%	90%	99%																					
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	15%	15%	15%	y	➤		➤		➤		➤		➤	y	➤						PCc_5kHzSelf_Test
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	15%	15%	y	➤		➤		➤		➤		➤	y	➤						PCc_5kHzSelf_Test
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	y	➤		➤		➤		➤		➤	y	➤						PCc_5kHzSelf_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y	➤		➤		➤		➤		➤	y	➤						PCc_5kHzSelf_Test
			Offsets	Offsets	5%	0%	0%		➤		➤		➤		➤		➤		➤						
		Stuck in range	Stuck in range	Stuck in range	10%	10%	10%	Y	➤		➤		➤		➤		➤	y	➤						PCc_5kHzSelf_Test
				Drift & Oscillation	5%	0%	0%		➤		➤		➤		➤		➤		➤						
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	5%	5%	5%	y													➤		➤	y	
			Drift	Drift & Oscillation	20%	20%	20%	y													➤		➤	y	
				Power Spikes	5%	5%	5%	y													➤		➤	y	
									0.00%		0.00%		0.00%		0.00%		59.40%		0.00%		0.00%		29.70%		

Appendix E5 – BMS – Architecture 5 DC% Claims

Table 153: BMS - Architecture 5 Actuator 5

Reference	5)A5	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			99.00%	High	99.00%	High	35.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 5								Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
										Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																		
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	20%	0%	0%			➤												
		Welded Contacts	Welded Contacts	Welded Contacts	5%	0%	0%			➤												
			Individual welded contacts	Individual welded contacts	10%	0%	0%			➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%					➤		➤								
			Drift	Drift & Oscillation	15%	0%	0%					➤		➤								
				Power Spikes	5%	0%	0%					➤		➤								
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	10%	10%	10%	y								➤	y	➤	y	➤	y	PCc_5kHzSelft_Test
				Incorrect action	15%	15%	15%	y								➤	y	➤	y	➤	y	PCc_5kHzSelft_Test
				Delayed Action	10%	10%	10%	y								➤	y	➤	y	➤	y	PCc_5kHzST_Monitor
										0.00%		0.00%		0.00%		21%		35%		35%		

Table 154: BMS - Architecture 5 Actuator 6

Reference	5)A6	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			99.00%	High	98.28%	Medium	55.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 5								Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
										Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																		
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	20%	0%	0%			➤												
		Welded Contacts	Welded Contacts	Welded Contacts	5%	0%	0%			➤												
			Individual welded contacts	Individual welded contacts	10%	0%	0%			➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y				➤		➤	y							PCc_PSU_Mon
			Drift	Drift & Oscillation	15%	15%	15%	y				➤		➤	y							PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y				➤		➤	y							PCc_PSU_Mon
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	10%	0%	0%									➤		➤		➤		
				Incorrect action	15%	15%	15%	y								➤		➤		➤	y	PCc_5kHzSelft_Test
				Delayed Action	10%	10%	10%	y								➤		➤		➤	y	PCc_5kHzST_Monitor
										0.00%		0.00%		29.70%		0%		0%		25%		

Table 155: BMS - Architecture 5 Connection 5

Reference	5)C5	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description Technique from ISO26262		Specific PCC
Table 26262-5: 2011		100%		99.00%	High	99.00%	High	40.00%	Failure Detection by on-line monitoring		
		Maintain Cells in Operating Area Architecture Candidate 5							High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%							
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	0%	0%		➤		
				Contact resistance	10%	0%	0%		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	0%	0%		➤		
			Short Circuit to Vbat	Short Circuit to Vbat	20%	20%	20%	y	➤	Y	PCc_5kHzSelf_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y	➤	Y	PCc_5kHzSelf_Test
				Resistive drift between pins / signal lines	10%	10%	10%	y	➤	Y	PCc_5kHzSelf_Test
									39.60%		

BMS - Architecture 5 Connection 6

Similar techniques as Architecture 5 Connection 5 so not shown.

Table 156: BMS - Architecture 5 Data 12 (subset 1)

Reference	5)D12	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description Technique from ISO26262										Specific PCC
Table 26262-5: 2011		100%		99.00%	High	96.03%	Medium	26.00%	Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		
		Maintain Cells in Operating Area Architecture Candidate 5							High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	
		Low 60%	Medium 90%	High 99%																	
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%		➤		➤		➤		➤		➤		➤		
			Offsets	Offsets	10%	0%	0%		➤		➤		➤				➤		➤		
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%		➤		➤		➤				➤		➤		
				Oscillation	4%	0%	0%		➤		➤		➤				➤		➤		
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	15%	14%	Y													PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time
		Message corruption	Message corruption	Message corruption	2%	2%	2%	Y													PCc_Data_Checksum
		Message Delay	Message Delay	Message Delay	3%	3%	3%	Y													PCc_Poll_Response_Time
		Message Loss	Message Loss	Message Loss	2%	2%	2%	Y													PCc_Frame_Seq
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	1%	1%	Y													PCc_Frame_Seq
			Resequencing	Resequencing	1%	1%	1%	Y													PCc_Frame_Seq
			Insertion of message	Insertion of message	1%	1%	1%	Y													PCc_Frame_Seq
				Masquerading	1%	1%	1%	Y													PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time.
									0.00%		0.00%		73.26%		0.00%		0.00%		0.00%		

Table 157: BMS - Architecture 5 Data 12 (subset 2)

Reference	5)D12	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			99.00%	High	96.03%	Medium	26.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 5								One-bit hardware redundancy	Multi-bit hardware redundancy	Read back of sent message	Complete hardware redundancy	Inspection using test patterns	Transmission redundancy	Information redundancy	PCc Frame Seq	Timeout monitoring	Combination of information Redundancy (rame count and timeout		
										Low 60%	Medium 90%	Medium 90%	High 99%	High 99%	Medium 90%	Medium 90%	Medium 90%	Medium 90%	High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.7.1	Used	D.2.7.2	Used	D.2.7.9	Used	D.2.7.3	Used	D.2.7.4	Used	D.2.7.5	Used	D.2.7.6	Used	D.2.7.7	Used	D.2.7.8	Used	D.2.7.6,7,8	Used	
		Low 60%	Medium 90%	High 99%																									
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	30%	0%	0%																						
			Offsets	Offsets	10%	0%	0%																						
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%																						
				Oscillation	4%	0%	0%																						
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	15%	15%	14%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time
		Message corruption	Message corruption	Message corruption	2%	2%	2%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Data_Checksum
		Message Delay	Message Delay	Message Delay	3%	3%	3%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Poll_Response_Time
		Message Loss	Message Loss	Message Loss	2%	2%	2%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Frame_Seq
		Unintended message repetition	Unintended message repetition	Unintended message repetition	1%	1%	1%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Frame_Seq
			Resequencing	Resequencing	1%	1%	1%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Frame_Seq
			Insertion of message	Insertion of message	1%	1%	1%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Frame_Seq
				Masquerading	1%	1%	1%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	y	PCc_Data_Checksum, PCc_Frame_Seq, PCc_Poll_Response_Time.
										0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		25.74%		

Table 158: BMS - Architecture 5 Measurement 5

Reference	5)M5	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			81.45%	Low	79.82%	Low	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 5								Failure Detection by on-line monitoring		Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		
										High 99%		Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	
		Low 60%	Medium 90%	High 99%																				
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines		0%	0%			➤	Y													
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit		0%	0%					➤		➤		➤		➤		➤		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	20%	20%	19%	Y				➤		➤		➤		➤		➤	y	➤		
			Short Circuit to Vbat	Short Circuit to Vbat	15%	15%	15%	Y				➤		➤		➤		➤		➤	y	➤		PCc_5kHzSelf_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	20%	20%	19%	Y				➤		➤		➤		➤		➤	y	➤		PCc_5kHzSelf_Test
			Offsets	Offsets	15%	9%	9%	Y				➤	y	➤		➤		➤		➤		➤		PCc_5kHzSelf_Test
		Stuck in range	Stuck in range	Stuck in range	20%	12%	12%	Y				➤	y	➤		➤		➤		➤		➤		PCc_5kHzSelf_Test
			Drift & Oscillation	Drift & Oscillation	10%	6%	6%	Y				➤	y	➤		➤		➤		➤		➤		PCc_5kHzSelf_Test
										0.00%		27.00%		0.00%		0.00%		0.00%		54.45%		0.00%		

Table 159: BMS - Architecture 5 Output 3

Reference	5)O3	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%			99.00%	High	98.26%	Medium	60.00%	Technique from ISO26262														
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 5								Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)	
										Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		Low 60%		High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																						
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	15%	0%	0%			>		>		>		>		>		>						
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%			>		>		>		>		>		>						
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	y		>	y	>		>		>		>	y	>						PCc_5kHzSelf_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y		>	y	>		>		>		>	y	>						PCc_5kHzSelf_Test
			Offsets	Offsets	5%	0%	0%			>		>		>		>		>		>						
		Stuck in range	Stuck in range	Stuck in range	10%	10%	10%	Y		>	y	>		>		>		>	y	>						PCc_5kHzSelf_Test
				Drift & Oscillation	5%	0%	0%			>		>		>		>		>		>						
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	5%	5%	5%	y														>		>	y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	y														>		>	y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y														>		>	y	PCc_PSU_Mon
										18.00%		0.00%		0.00%		0.00%		29.70%		0.00%		0.00%		29.70%		

Table 160: BMS - Architecture 5 Transducer 3

Reference	5)T3	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%			99.00%	High	97.54%	Medium	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 5								Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Voltage or current control (input)		Voltage or current control (output)	
										High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		Low 60%		High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																						
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	20%	19%	y		>	y	>		>		>		>		>						PCc6801_Self_-Test, PCc_5kHzSelf_Test
			Offsets	Offsets	10%	10%	10%	y		>	y	>		>		>		>		>						PCc6801_Self_-Test, PCc_5kHzSelf_Test
		Stuck in range	Stuck in range	Stuck in range	30%	30%	29%	y		>	Y	>		>		>		>		>						PCc6801_Self_-Test, PCc_5kHzSelf_Test
				Oscillation	5%	5%	5%	y		>	Y	>		>		>		>		>						PCc6801_Self_-Test, PCc_5kHzSelf_Test
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y														>		>	y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	y														>		>	y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y														>		>	y	PCc_PSU_Mon
										64.35%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		34.65%		

Table 161: BMS - Architecture 5 Transducer 4

Reference	5)T4	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%			81.45%	Low	80.34%	Low	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 5								Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Voltage or current control (input)		Voltage or current control (output)	
										High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		Low 60%		High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																						
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	20%	19%	y		>	y	>		>		>		>		>						PCc_5kHzSelf_Test
			Offsets	Offsets	10%	6%	6%	y		>		>		>		>	y	>		>						PCc_5kHzSelf_Test
		Stuck in range	Stuck in range	Stuck in range	30%	18%	18%	y		>		>		>		>	y	>		>						PCc_5kHzSelf_Test
				Oscillation	5%	3%	3%	y		>		>		>		>	y	>		>						PCc_5kHzSelf_Test
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y														>		>	y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	y														>		>	y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y														>		>	y	PCc_PSU_Mon
										19.80%		0.00%		0.00%		27.00%		0.00%		0.00%		0.00%		34.65%		

Table 162: BMS - Architecture 6 Actuator 1

Reference	6)A1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
Table 26262-5: 2011		100%		83.83%	Low	83.39%	Low	90.00%	Technique from ISO26262										
		Maintain Cells in Operating Area Architecture Candidate 6							Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
									Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																	
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	20%	12%	12%	y	➤	Y											PCc_HVPosBatt
		Welded Contacts	Welded Contacts	Welded Contacts	5%	3%	3%	y	➤	Y											PCc_HVPosBatt
			Individual welded contacts	Individual welded contacts	10%	6%	6%	y	➤	Y											PCc_HVPosBatt
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y			➤		➤	y							PCc_PSU_Mon
			Drift	Drift & Oscillation	15%	15%	15%	y			➤		➤	y							PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y			➤		➤	y							PCc_PSU_Mon
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	10%	0%	0%								➤		➤		➤		
				Incorrect action	15%	15%	15%	y							➤		➤		➤	Y	PCc_HVPosBatt
				Delayed Action	10%	10%	10%	y							➤		➤		➤	Y	PCc_HVPosBatt
									21.00%		0.00%		29.70%		0%		0%		25%		

BMS - Architecture 6 Actuator 2

Similar techniques as Architecture 6 Actuator 1 so not shown.

BMS - Architecture 6 Actuator 4

Similar techniques as Architecture 6 Actuator 1 so not shown.

BMS - Architecture 6 Actuator 7

Similar techniques as Architecture 6 Actuator 1 so not shown.

Table 163: BMS - Architecture 6 Connection 1

Reference	6)C1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			99.00%	High	99.00%	High	100.00%	Technique from ISO26262		
		Maintain Cells in Operating Area Architecture Candidate 6								Failure Detection by on-line monitoring High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	20%	20%	y		➤	Y	PCc_6803_Self_Test
				Contact resistance	10%	10%	10%	y		➤	Y	PCc_HVPosBatt
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	30%	30%	y		➤	Y	PCc_6803_Self_Test
			Short Circuit to Vbat	Short Circuit to Vbat	20%	20%	20%	y		➤	Y	PCc_6803_Self_Test
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y		➤	Y	PCc_6803_Self_Test
				Resistive drift between pins / signal lines	10%	10%	10%	y		➤	Y	PCc_HVPosBatt
										99.00%		

BMS - Architecture 6 Connection 2

Similar techniques as Architecture 6 Connection 1 so not shown.

Table 164: BMS - Architecture 6 Measurement 1

Reference	6)M1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%		99.00%	High	98.58%	Medium	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 6							Failure Detection by on-line monitoring		Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		
									High 99%		Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	
		Low 60%	Medium 90%	High 99%																			
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	15%	15%	Y	➤	Y													PCc_HVPosBatt
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	10%	10%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_OA_Window, PCc_6803_Self_Test, PCc6801_Self_-Test, PCc_HVPosBatt
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	15%	15%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_OA_Window, PCc_6803_Self_Test, PCc6801_Self_-Test, PCc_HVPosBatt
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_OA_Window, PCc_6803_Self_Test, PCc6801_Self_-Test, PCc_HVPosBatt
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_OA_Window, PCc_6803_Self_Test, PCc6801_Self_-Test, PCc_HVPosBatt
			Offsets	Offsets	15%	15%	15%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_OA_Window, PCc_6803_Self_Test, PCc6801_Self_-Test, PCc_HVPosBatt
		Stuck in range	Stuck in range	Stuck in range	15%	15%	15%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_OA_Window, PCc_6803_Self_Test, PCc6801_Self_-Test, PCc_HVPosBatt
			Drift & Oscillation	Drift & Oscillation	10%	10%	10%	Y			➤	Y	➤		➤		➤		➤	y	➤	Y	PCc_OA_Window, PCc_6803_Self_Test, PCc6801_Self_-Test, PCc_HVPosBatt
									14.85%		51.00%		0.00%		0.00%		0.00%		84.15%		84.15%		

Table 165: BMS - Architecture 6 Measurement 3

Reference	6)M3	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%		99.00%	High	98.58%	Medium	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 6							Failure Detection by on-line monitoring		Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		
									High 99%		Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	
		Low 60%	Medium 90%	High 99%																			
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	15%	15%	Y	➤	Y													
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	10%	10%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_HW_MONITOR, PCc_HVPosBatt
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	15%	15%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_HW_MONITOR, PCc_HVPosBatt
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_HW_MONITOR, PCc_HVPosBatt
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_HW_MONITOR, PCc_HVPosBatt
			Offsets	Offsets	15%	15%	15%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_HW_MONITOR, PCc_HVPosBatt
		Stuck in range	Stuck in range	Stuck in range	15%	15%	15%	Y			➤	Y	➤		➤		➤		➤	Y	➤	Y	PCc_HW_MONITOR, PCc_HVPosBatt
			Drift & Oscillation	Drift & Oscillation	10%	10%	10%	Y			➤	Y	➤		➤		➤		➤	y	➤	Y	PCc_HW_MONITOR, PCc_HVPosBatt
									14.85%		51.00%		0.00%		0.00%		0.00%		84.15%		84.15%		

Table 166: BMS - Architecture 6 Output 1

Reference	6)O1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		99.00%	High	98.26%	Medium	60.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 6							Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		
									Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		Low 60%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																					
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	15%	0%	0%																		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%																		
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	y		y								y							PCc_HVPosBatt
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y		y								y							PCc_HVPosBatt
			Offsets	Offsets	5%	0%	0%																		
		Stuck in range	Stuck in range	Stuck in range	10%	10%	10%	Y		y								y							PCc_HVPosBatt
				Drift & Oscillation	5%	0%	0%																		
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	5%	5%	5%	y																y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	y																y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y																y	PCc_PSU_Mon
									18.00%		0.00%		0.00%		0.00%		29.70%		0.00%		0.00%		29.70%		

BMS - Architecture 6 Output 2

Similar techniques as Architecture 6 Output 1 so not shown.

BMS - Architecture 6 Output 5

Similar techniques as Architecture 6 Output 1 so not shown.

BMS - Architecture 6 Output 6

Similar techniques as Architecture 6 Output 1 so not shown.

Table 167: BMS - Architecture 6 Transducer 1

Reference	6)T1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%		99.00%	High	97.94%	Medium	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 6							Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Voltage or current control (input)		Voltage or current control (output)		
									High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		Low 60%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																					
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	20%	20%	y		y				Y		y									PCc_OA_Window, PCc_6803_Self_Test, PCc_HVPosBatt
			Offsets	Offsets	10%	10%	10%	y		y				Y											PCc_6803_Self_Test, PCc_HVPosBatt
		Stuck in range	Stuck in range	Stuck in range	30%	30%	29%	y						Y											PCc_HVPosBatt
				Oscillation	5%	5%	5%	y						Y											PCc_HVPosBatt
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y																y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	y																y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y																y	PCc_PSU_Mon
									29.70%		0.00%		64.35%		12.00%		0.00%		0.00%		0.00%		34.65%		

Table 168: BMS - Architecture 6 Transducer 3

Reference	6)T3	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												
		100%			99.00%	High	98.18%	Medium	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 6								Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Voltage or current control (input)		Voltage or current control (output)		Specific PCC
										High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		Low 60%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																						
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	20%	20%	y		➤	y	➤		➤	y	➤				➤						PCc6801_Self_-Test, PCc_5kHzSelf_Test, PCc_HVPosBatt
			Offsets	Offsets	10%	10%	10%	y		➤	y	➤		➤	y	➤		➤		➤						PCc6801_Self_-Test, PCc_5kHzSelf_Test, PCc_HVPosBatt
		Stuck in range	Stuck in range	Stuck in range	30%	30%	29%	y		➤	Y	➤		➤	y	➤		➤		➤						PCc6801_Self_-Test, PCc_5kHzSelf_Test, PCc_HVPosBatt
				Oscillation	5%	5%	5%	y		➤	Y	➤		➤	y	➤		➤		➤						PCc6801_Self_-Test, PCc_5kHzSelf_Test, PCc_HVPosBatt
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y														➤		➤	y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	y														➤		➤	y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y														➤		➤	y	PCc_PSU_Mon
										64.35%		0.00%		64.35%		0.00%		0.00%		0.00%		0.00%		34.65%		

Appendix E7 – BMS – Architecture 7 DC% Claims

Table 169: BMS - Architecture 7 Actuator 1

Reference	7)A1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%		85.35%	Low	84.86%	Low	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 7							Failure Detection by on-line monitoring		Voltage or current control (input)	Voltage or current control (output)	Failure Detection by on-line monitoring		Test Pattern		Monitoring		
									Low		Low	High	Low		High		High		
									60%		60%	99%	60%		99%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low	Medium	High																	
		60%	90%	99%																	
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	20%	12%	12%	Y	➤	Y											PCc_HVPosBatt
		Welded Contacts	Welded Contacts	Welded Contacts	5%	3%	3%	Y	➤	Y											PCc_HVPosBatt
			Individual welded contacts	Individual welded contacts	10%	6%	6%	Y	➤	Y											PCc_HVPosBatt
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y			➤		➤	y							PCc_PSU_Mon
			Drift	Drift & Oscillation	15%	15%	15%	y			➤		➤	y							PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y			➤		➤	y							PCc_PSU_Mon
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	0%	0%	0%								➤		➤		➤		
				Incorrect action	20%	20%	20%	y							➤		➤		➤	y	PCc_HVPosBatt
				Delayed Action	15%	15%	15%	y							➤		➤		➤	y	PCc_HVPosBatt
									21.00%		0.00%	29.70%	0%		0%		35%				

BMS - Architecture 7 Actuator 2

Similar techniques as Architecture 7 Actuator 1 so not shown.

BMS - Architecture 7 Actuator 4

Similar techniques as Architecture 7 Actuator 1 so not shown.

BMS - Architecture 7 Actuator 7

Similar techniques as Architecture 7 Actuator 1 so not shown.

Table 170: BMS - Architecture 7 Output 1

Reference	7)O1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%		99.00%	High	98.51%	Medium	60.00%	Technique from ISO26262														
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 7							Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		
									Low		High		Medium		High		High		High		Low		High		
									60%		99%		90%		99%		99%		99%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																					
		60%	90%	99%																					
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	15%	0%	0%		➤		➤		➤		➤		➤		➤						
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%		➤		➤		➤		➤		➤		➤						
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	y	➤	y	➤	y	➤		➤		➤	y	➤						PCc_HVPosBatt, PCc_POSCON
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	y	➤	y	➤	y	➤		➤		➤	y	➤						PCc_HVPosBatt, PCc_POSCON
			Offsets	Offsets	5%	0%	0%		➤		➤		➤		➤		➤		➤						
		Stuck in range	Stuck in range	Stuck in range	10%	10%	10%	Y	➤	y	➤	y	➤		➤		➤	y	➤						PCc_HVPosBatt, PCc_POSCON
				Drift & Oscillation	5%	0%	0%		➤		➤		➤		➤		➤		➤						
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	5%	5%	5%	y													➤		➤	y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	y													➤		➤	y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y													➤		➤	y	PCc_PSU_Mon
									18.00%		29.70%		0.00%		0.00%		29.70%		0.00%		0.00%		29.70%		

BMS - Architecture 7 Output 2

Similar techniques as Architecture 7 Output 1 so not shown.

BMS - Architecture 7 Output 5

Similar techniques as Architecture 7 Output 1 so not shown.

BMS - Architecture 7 Output 6

Similar techniques as Architecture 7 Output 1 so not shown.

Safety Goal: Maintain Voltage Operating Area										SPFM Calculation for Architecture 7			
		Total FR (FIT)		431.57						Residual or Single Point (FIT)			12.5435
										Single Point Fault Metric			97.09%
System	Sub System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point Fault failure rate / FIT
Cell / Battery Management	uC, Xtal and supply decouplings	U9	YES	3	All	50%	X	1.500	uC stops working	SM12	Wdog	90%	0.1500
					All	50%		0.000	Failures do not violate safety goal				0.0000
		X1	YES	0.4404	Open	89%	X	0.392	uC stops working	SM12	Wdog	90%	0.0392
					No oscillation	11%	X	0.048	uC stops working	SM12	Wdog	90%	0.0048
		C92	YES	0.0585	Short	49%	X	0.029	Crystal does not oscillate correctly, uC stops	SM12	Wdog	90%	0.0029
					Open	22%	X	0.013	Crystal does not oscillate correctly, uC stops	SM12	Wdog	90%	0.0013
					Value change	29%	X	0.017	Crystal does not oscillate correctly, uC stops	SM12	Wdog	90%	0.0017
		C94	YES	0.0585	Short	49%	X	0.029	Crystal does not oscillate correctly, uC stops	SM12	Wdog	90%	0.0029
					Open	22%	X	0.013	Crystal does not oscillate correctly, uC stops	SM12	Wdog	90%	0.0013
					Value change	29%	X	0.017	Crystal does not oscillate correctly, uC stops	SM12	Wdog	90%	0.0017
		R175	YES	0.8564	Short	5%	X	0.043	Crystal does not oscillate correctly, uC stops	SM2	CAN	99%	0.0004
					Open	59%	X	0.505	Crystal does not oscillate correctly, uC stops	SM2	CAN	99%	0.0051
					Value change	36%		0.000		SM2	CAN	99%	0.0000
		C98	YES	0.489	Short	49%	X	0.240	uC core voltage 0, uC held in reset	SM2	CAN	99%	0.0024
					Open	22%	X	0.108	uC core voltage incorrect, uC unstable	SM2	CAN	99%	0.0011
					Value change	29%		0.000	uC core voltage not affected by value change				0.0000
		C100	YES	0.2009	Short	49%	X	0.098	uC core voltage 0, uC held in reset	SM2	CAN	99%	0.0010
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
		C91	YES	0.2009	Short	49%	X	0.098	uC core voltage 0, uC held in reset	SM2	CAN	99%	0.0010
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
		C84	YES	0.2009	Short	49%	X	0.098	uC core voltage 0, uC held in reset	SM2	CAN	99%	0.0010
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
		C90	YES	0.2009	Short	49%	X	0.098	uC core voltage 0, uC held in reset	SM2	CAN	99%	0.0010
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
		C96	YES	0.2009	Short	49%	X	0.098	uC core voltage 0, uC held in reset	SM2	CAN	99%	0.0010
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
	uC ADC Vdd Supply	L1	YES	0.3828	Short	42%	X	0.161	ADC Vdd noisy as connected to Digital				0.1608
					Open	42%	X	0.161	Loss of ADC Vdd				0.1608
					Value change	16%	X	0.061	Noisy ADC Vdd				0.0612
		C87	YES	0.2009	Short	49%	X	0.098	uC core voltage 0, uC held in reset	SM2	CAN	99%	0.0010
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
		C107	YES	0.2009	Short	49%	X	0.098	uC core voltage 0, uC held in reset	SM2	CAN	99%	0.0010
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
	uC ADC Vref	C85	YES	0.2009	Short	49%	X	0.098	uC core voltage 0, uC held in reset	SM2	CAN	99%	0.0010
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
		C89	YES	0.5696	Short	49%	X	0.279	uC core voltage 0, uC held in reset	SM2	CAN	99%	0.0028
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
		U17	YES	2.1	All	50%	X	1.050	Incorrect ADC scaling	SM14	PCc ADref	99%	0.0105
					All	50%		0.000					0.0000
	uC	U?	NO	0	All	50%		0.000	Failures do not violate safety goal				0.0000

Battery Pack SPFM Calculations Sheet 1 of 38

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
	Program				All	50%		0.000					0.0000
	uC Reset	R132	YES	0.7785	Short	5%	X	0.039	Fast reset	SM2	CAN	99%	0.0004
					Open	59%	X	0.459	Held in reset	SM2	CAN	99%	0.0046
					Value change	36%	X	0.280	Possible incorret reset	SM2	CAN	99%	0.0028
		C93	YES	0.1455	Short	49%	X	0.071	Held in reset	SM2	CAN	99%	0.0007
					Open	22%	X	0.032	Fast reset	SM2	CAN	99%	0.0003
					Value change	29%	X	0.042	Possible incorret reset	SM2	CAN	99%	0.0004
	External flash memory	R136	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R140	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		U7	NO	0				0.000					0.0000
								0.000					0.0000
		C81	NO	0	Short	49%	X	0.000	+3.3V supply shorted to ground	SM2	CAN	99%	0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
		R137	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	uC LED	LED13	NO	0				0.000					0.0000
								0.000					0.0000
		R156	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	5V supply potential divider to ADC	R159	NO	0	Short	5%		0.000	Failures do not violate safety goal				0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R154	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C99	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	3V3 supply potential divider to ADC	R157	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R158	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C76	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	uC temperature measurement to ADC	R138	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R135	NO	0	Short	15%		0.000					0.0000
					Open	63%		0.000					0.0000
					Value change	22%		0.000					0.0000
		C77	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		U15	YES	0.9	All	50%	X	0.450	CAN does not function	SM2	CAN	99%	0.0045
					All	50%		0.000	Failures do not violate safety goal				0.0000
		C132	YES	0.0618	Short	49%	X	0.030	CAN-L shorted to GND	SM2	CAN	99%	0.0003
			YES		Open	22%		0.000					0.0000
			YES		Value change	29%		0.000					0.0000
		C133	YES	0.0618	Short	49%	X	0.030	CAN-H shorted to GND	SM2	CAN	99%	0.0003
			YES		Open	22%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point Fault failure rate / FIT
	CAN		YES		Value change	29%		0.000					0.0000
		L5	YES	0.0011	Short	42%	X	0.000	CAN does not function	SM2	CAN	99%	0.0000
			YES		Open	42%	X	0.000	CAN does not function	SM2	CAN	99%	0.0000
			YES		Value change	16%		0.000					0.0000
		D66A	YES	2.34	Short	20%	X	0.468	CAN-H shorted to GND	SM2	CAN	99%	0.0047
			YES		Open	45%		0.000					0.0000
			YES		Value change	35%		0.000					0.0000
		D66B	YES	2.34	Short	20%	X	0.468	CAN-L shorted to GND	SM2	CAN	99%	0.0047
			YES		Open	45%		0.000					0.0000
			YES		Value change	35%		0.000					0.0000
		C131	YES	0.0645	Short	20%	X	0.013	+5V supply shorted to 0V	SM2	CAN	99%	0.0001
			YES		Open	51%		0.000	Can May become unreliable				0.0000
			YES		Value change	29%		0.000					0.0000
		C129	YES	0.2773	Short	20%	X	0.055	+3.3V supply shorted to ground	SM2	CAN	99%	0.0006
			YES		Open	51%		0.000	Can May become unreliable				0.0000
			YES		Value change	29%		0.000					0.0000
		C130	YES	0.2009	Short	49%	X	0.098	+3.3V supply shorted to ground	SM2	CAN	99%	0.0010
			YES		Open	22%		0.000					0.0000
			YES		Value change	29%		0.000					0.0000
		J1-5	YES	0.0081	All	50%	X	0.004	CAN-H line broken/shorted	SM2	CAN	99%	0.0000
			YES		All	50%		0.000	Failures do not violate safety goal				0.0000
		J1-1	YES	0.0081	All	50%	X	0.004	CAN-L line broken/shorted	SM2	CAN	99%	0.0000
			YES		All	50%		0.000	Failures do not violate safety goal				0.0000
	6803 Cell Voltage Measurement	U1	YES	20.81	All	50%	X	10.405	6803 does not function correctly	SM19	6803SelfTest	99%	0.1041
			YES		All	50%		0.000	Failures do not violate safety goal				0.0000
		R30	YES	0.75	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.442	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0044
					Value change	36%		0.000	Negligible effect on EMC performance				0.0000
		C9	YES	0.2009	Short	49%	X	0.098	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0010
					Open	22%	X	0.044	Degraded EMC performance				0.0442
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
		D8	YES	13.997	Short	49%		0.000	Reduced negative transient immunity				0.0000
					Open	36%	X	5.039	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0504
					Value change	15%		0.000	Negligible effect				0.0000
		Q4	YES	1.2096	Short	51%		0.000	6803 always powered, no standby mode				0.0000
					Open	5%	X	0.060	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%	X	0.266	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0027
					Output high	5%		0.000	6803 always powered, no standby mode				0.0000
		R35	YES	2.3096	Short	5%	X	0.115	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0012
					Open	59%		0.000					0.0000
					Value change	36%		0.000	Negligible effect				0.0000
		R32	YES	0.9387	Short	5%		0.000					0.0000
					Open	59%	X	0.554	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0055
					Value change	36%		0.000	Negligible effect				0.0000
		Q5	YES	1.2096	Short	51%		0.000	6803 always powered, no standby mode				0.0000
					Open	5%	X	0.060	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	6803 always powered, no standby mode				0.0000

Battery Pack SPFM Calculations Sheet 3 of 38

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Output high	5%	X	0.060	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0006
		C12	YES	0.2009	Short	49%	X	0.098	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0010
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000	Negligible effect				0.0000
		R38	YES	2.3096	Short	5%	X	0.115	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0012
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R40	YES	0.8108	Short	5%		0.000					0.0000
					Open	59%	X	0.478	No power to 6803, no LTC V measurements	SM4	SPI Data Checks	99%	0.0048
					Value change	36%		0.000					0.0000
		R13	YES	0.8564	Short	5%	X	0.043	6803 cannot reset on watchdog timeout	SM4	SPI Data Checks	99%	0.0004
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C5	YES	0.5696	Short	49%	X	0.279	Vreg output short to GND	SM4	SPI Data Checks	99%	0.0028
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R11	NO	0	Short	5%		0.000	Pullup on unused GPIO pin				0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C6	YES	0.5696	Short	49%	X	0.279	Vref output short to GND	SM5	Vref Check	60%	0.1116
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	6803 Temp Measurement (on PCB)	R14	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R1	NO	0	Short	15%		0.000					0.0000
					Open	63%		0.000					0.0000
					Value change	22%		0.000					0.0000
		C2	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	6803 Cell Measurement SPI Comms (pull ups and series resistors)	R16	YES	0.9387	Short	5%	X	0.047	CS comms line pulled high	SM4	SPI Data Checks	99%	0.0005
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R24	YES	0.9387	Short	5%	X	0.047	SDI comms line pulled high	SM4	SPI Data Checks	99%	0.0005
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R23	YES	0.9387	Short	5%	X	0.047	CLOCK comms line pulled high	SM4	SPI Data Checks	99%	0.0005
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R17	YES	0.8108	Short	5%		0.000					0.0000
					Open	59%	X	0.478	CS comms line open circuit	SM4	SPI Data Checks	99%	0.0048
					Value change	36%		0.000					0.0000
		R15	YES	0.8108	Short	5%		0.000					0.0000
					Open	59%	X	0.478	SDO comms line open circuit	SM4	SPI Data Checks	99%	0.0048
					Value change	36%		0.000					0.0000
		R26	YES	0.8108	Short	5%		0.000					0.0000
					Open	59%	X	0.478	SDI comms line open circuit	SM4	SPI Data Checks	99%	0.0048
					Value change	36%		0.000					0.0000
		R25	YES	0.8108	Short	5%		0.000					0.0000
					Open	59%	X	0.478	CLOCK comms line open circuit	SM4	SPI Data Checks	99%	0.0048
					Value change	36%		0.000					0.0000
		R141	YES	0.7785	Short	5%	X	0.039	SDO comms line pulled high	SM4	SPI Data Checks	99%	0.0004
					Open	59%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	36%		0.000					0.0000
	6803 Temperature to uC ADC Filter	R5	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C97	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	6803 Vref to uC ADC Filter	R7	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C101	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	Cell 12 clamp voltage	L3	YES	0.3828	Short	42%		0.000	Reduced transient immunity				0.0000
					Open	42%	X	0.161	No power to 6803	SM19	6803SelfTest	99%	0.0016
					Value change	16%		0.000	Negligible effect				0.0000
		C120	YES	0.6945	Short	49%	X	0.340	Cell 12 short to GND, no power to 6803	SM19	6803SelfTest	99%	0.0034
					Open	22%		0.000	Reduced transient and EMC immunity				0.0000
					Value change	29%		0.000	Negligible effect on EMC performance				0.0000
		D64	YES	13.997	Short	49%	X	6.858	Cell 12 short to GND, no power to 6803	SM19	6803SelfTest	99%	0.0686
					Open	36%		0.000	Reduced negative transient immunity				0.0000
					Value change	15%		0.000	Negligible effect				0.0000
		D63	YES	13.997	Short	49%	X	6.858	Cell 12 short to GND, no power to 6803	SM19	6803SelfTest	99%	0.0686
					Open	36%		0.000	Reduced negative transient immunity				0.0000
					Value change	15%		0.000	Negligible effect				0.0000
		D62	YES	0.72	Short	49%	X	0.353	Cell 12 short to GND, no power to 6803	SM19	6803SelfTest	99%	0.0035
					Open	36%		0.000	Reduced positive transient immunity				0.0000
					Value change	15%		0.000	Negligible effect				0.0000
		R176	NO	0	Short	49%		0.000	Not Fitted				0.0000
					Open	36%		0.000	Not Fitted				0.0000
					Value change	15%		0.000	Not Fitted				0.0000
		R177	YES	0.001	Short	49%		0.000	nominal value				0.0000
					Open	36%	X	0.000	Reduced positive transient immunity				0.0004
					Value change	15%		0.000	Negligible effect				0.0000
	Cell 12 Filter	R172	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R82	YES	0.727	Short	5%	X	0.036	Cell discharge current not limited	SM19	6803SelfTest	99%	0.0004
					Open	59%	X	0.429	Cell only discharges slowly through LED				0.4289
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED12	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R97	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q22	YES	1.2096	Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D36	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R98	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C117	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D57	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
	Cell 11 Filter	R171	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R100	YES	0.727	Short	5%	X	0.036	Cell discharge current not limited	SM19	6803SelfTest	99%	0.0004
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED11	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R102	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q16	YES	1.2096	Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D34	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R86	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C112	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D56	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R88	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R105	YES	0.727	Short	5%		0.000	Cell discharge current not limited				0.0000
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED10	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R107	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q15	YES	1.2096	Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
	Filter				Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D33	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R73	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C104	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D55	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R170	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R111	YES	0.727	Short	5%		0.000	Cell discharge current not limited				0.0000
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED9	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R114	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	Cell 9 Filter	Q14	YES	1.2096	Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D32	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R72	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C103	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D54	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R61	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R128	YES	0.727	Short	5%		0.000	Cell discharge current not limited				0.0000
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED8	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R143	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
					Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
	Cell 8 Filter	Q8	YES	1.2096	Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D22	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R60	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C102	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D53	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
	Cell 7 Filter	R129	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R153	YES	0.727	Short	5%		0.000	Cell discharge current not limited				0.0000
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED7	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R155	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q35	YES	1.2096	Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D52	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R151	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C11	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D7	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R48	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R58	YES	0.727	Short	5%		0.000	Cell discharge current not limited				0.0000
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED6	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R78	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
					Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
	Cell 6 Filter	Q34	YES	1.2096	Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D51	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R148	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C10	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D6	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R34	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R83	YES	0.727	Short	5%		0.000	Cell discharge current not limited				0.0000
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED5	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R99	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	Cell 5 Filter	Q31	YES	1.2096	Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D50	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R134	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C8	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D5	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R31	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R101	YES	0.727	Short	5%		0.000	Cell discharge current not limited				0.0000
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED4	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R103	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
	Cell 4 Filter	Q30	YES	1.2096	Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D49	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R130	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C7	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D4	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
	Cell 3 Filter	R10	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R106	YES	0.727	Short	5%		0.000	Cell discharge current not limited				0.0000
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED3	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R108	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q28	YES	1.2096	Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D43	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R119	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C3	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D1	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R4	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R112	YES	0.727	Short	5%		0.000	Cell discharge current not limited				0.0000
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED2	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R115	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	36%		0.000					0.0000
	Cell 2 Filter	Q27	YES	1.2096	Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D39	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R113	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C1	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D2	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
			YES		Open	45%		0.000					0.0000
			YES		Value change	35%		0.000					0.0000
	Cell 1 Filter	R2	YES	0.8108	Short	5%		0.000	Degraded EMC performance				0.0000
					Open	59%	X	0.478	6803 cannot measure cell voltage	SM19	6803SelfTest	99%	0.0048
					Value change	36%		0.000	Negligible effect				0.0000
		R131	YES	0.727	Short	5%		0.000	Cell discharge current not limited				0.0000
					Open	59%	X	0.429	Cell only discharges slowly through LED	SM19	6803SelfTest	99%	0.0043
					Value change	36%		0.000	Cell discharge current varies slightly				0.0000
		LED1	NO	0	Open	70%		0.000					0.0000
					Short	30%		0.000					0.0000
		R149	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q26	YES	1.2096	Short	51%	X	0.617	Cell permanently discharging	SM19	6803SelfTest	99%	0.0062
					Open	5%	X	0.060	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0006
					Value change	17%		0.000	Negligible effect				0.0000
					Output low	22%		0.000	No effect, since device used in saturation mode				0.0000
					Output high	5%		0.000	No effect, since device used in saturation mode				0.0000
		D38	YES	0.72	Short	20%	X	0.144	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R109	YES	0.7952	Short	5%		0.000					0.0000
					Open	59%	X	0.469	Cell cannot be discharged	SM19	6803SelfTest	99%	0.0047
					Value change	36%		0.000					0.0000
		C4	YES	1.3233	Short	49%		0.000	Cell temporarily shorted to GND				0.0000
					Open	22%		0.000	Degraded EMC performance				0.0000
					Value change	29%		0.000					0.0000
		D3	YES	0.72	Short	20%	X	0.144	Cell voltage cannot be measured	SM19	6803SelfTest	99%	0.0014
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		J4-1	YES	0.0562	All	50%	X	0.028	Ground Connection lost	Sm22	c 6803 Self Test HVF	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-2	YES	0.0562	All	50%	X	0.028	Cell 1 Connection to cell lost	SM22	c 6803 Self Test HVF	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-3	YES	0.0562	All	50%	X	0.028	Cell 3 Connection to cell lost	SM22	c 6803 Self Test HVF	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-4	YES	0.0562	All	50%	X	0.028	Cell 5 Connection to cell lost	SM22	c 6803 Self Test HVF	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-5	YES	0.0562	All	50%	X	0.028	Cell 7 Connection to cell lost	SM22	c 6803 Self Test HVF	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-6	YES	0.0562	All	50%	X	0.028	Cell 9 Connection to cell lost	SM22	c 6803 Self Test HVF	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
	Cell connections	J4-7	YES	0.0562	All	50%	X	0.028	Cell 11 Connection to cell lost	SM22	c 6803 Self Test HVR	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-8	YES	0.0562	All	50%	X	0.028	Power Connection lost	SM22	c 6803 Self Test HVR	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-9	NO	0	All	50%		0.000	Temperature Failures do not violate safety goal				0.0000
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-10	YES	0.0562	All	50%	X	0.028	Cell 0 (0v sense) Connection lost	SM22	c 6803 Self Test HVR	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-11	YES	0.0562	All	50%	X	0.028	Cell 2 Connection to cell lost	SM22	c 6803 Self Test HVR	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-12	YES	0.0562	All	50%	X	0.028	Cell 4 Connection to cell lost	SM22	c 6803 Self Test HVR	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-13	YES	0.0562	All	50%	X	0.028	Cell 6 Connection to cell lost	SM22	c 6803 Self Test HVR	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-14	YES	0.0562	All	50%	X	0.028	Cell 8 Connection to cell lost	SM22	c 6803 Self Test HVR	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-15	YES	0.0562	All	50%	X	0.028	Cell 10 Connection to cell lost	SM22	c 6803 Self Test HVR	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
		J4-16	YES	0.0562	All	50%	X	0.028	Cell 12 Connection to cell lost	SM22	c 6803 Self Test HVR	99%	0.0003
					All	50%		0.000	Failures do not violate safety goal				0.0000
	DC-DC Converter Power CBM from Cell stack (Battery Supply)	R168	NO	0	Short	5%		0.000	Failure of HV power supply does not effect operation, since everything can run off the LV power supply. Failures can be detected since micro measures 5Vdcdc rail voltage, which will be <5V when DC-DC PSU is not running due to voltage drop on D35				0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R169	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		L4	NO	0	Short	42%		0.000					0.0000
					Open	42%		0.000					0.0000
					Value change	16%		0.000					0.0000
		C125	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C126	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C127	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R167	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C123	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R165	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C122	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		U13	NO	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		C121	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D65	NO	0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C124	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R166	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	36%		0.000					0.0000
		R164	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		L2	NO	0	Short	42%		0.000					0.0000
					Open	42%		0.000					0.0000
					Value change	16%		0.000					0.0000
		C118	NO	0	Short	49%	X	0.000	5V dcdc rail short to GND, no 3.3V supply	SM2	CAN	99%	0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C119	NO	0	Short	49%	X	0.000	5V dcdc rail short to GND, no 3.3V supply	SM2	CAN	99%	0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	5V Power Supply	C136	YES	0.0645	Short	49%	X	0.032	VIN_SI_V_EB supply shorted to 0V, no	SM2	CAN	99%	0.0003
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C79	YES	0.2009	Short	57%	X	0.114	VIN_SI_V_EB supply shorted to 0V, no 5V supply	SM2	CAN	99%	0.0011
					Open	32%		0.000					0.0000
					Value change	11%		0.000					0.0000
		U16	YES	10	All	50%	X	5.000	+5V rail incorrect, no 3.3V supply	SM2	CAN	99%	0.0500
					All	50%		0.000	Failures do not violate safety goal				0.0000
		C135	YES	0.0645	Short	57%	X	0.037	LV supply shorted to 0V, no 3.3V supply	SM2	CAN	99%	0.0004
					Open	32%		0.000					0.0000
					Value change	11%		0.000					0.0000
		C88	YES	0.2009	Short	57%	X	0.114	VIN_SI_V_EB supply shorted to 0V, no 5V supply	SM2	CAN	99%	0.0011
					Open	32%		0.000					0.0000
					Value change	11%		0.000					0.0000
		L6	YES	0.0011	Short	42%		0.000					0.0000
					Open	42%	X	0.000	LV supply disconnected, no 3.3V supply	SM2	CAN	99%	0.0000
					Value change	16%		0.000					0.0000
		C59	YES	0.2009	Short	49%	X	0.098	LV supply shorted to 0V, no 3.3V	SM2	CAN	99%	0.0010
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		U3	YES	3	All	50%	X	1.500	+5Vdcdc rail incorrect, no 3.3V supply	SM2	CAN	99%	0.0150
					All	50%		0.000	Failures do not violate safety goal				0.0000
	5V Isolated Supply	C60	YES	0.387	Short	49%	X	0.190	LV supply shorted to 0V, no 3.3V supply	SM2	CAN	99%	0.0019
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C58	YES	0.387	Short	49%	X	0.190	LV supply shorted to GND, no 3.3V supply	SM2	CAN	99%	0.0019
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D35	YES	13.997	Short	49%		0.000					0.0000
					Open	36%	X	5.039	LV supply disconnected, no 3.3V supply	SM2	CAN	99%	0.0504
					Value change	15%		0.000					0.0000
		C110	YES	0.2773	Short	49%	X	0.136	LV supply shorted to GND, no 3.3V	SM2	CAN	99%	0.0014
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		U11	YES	0.4432	All	50%	X	0.222	No 3.3V supply	SM2	CAN	99%	0.0022
					All	50%		0.000	Failures do not violate safety goal				0.0000
	3V3 Power				Short	49%	X	0.098	3.3V rail shorted to GND	SM2	CAN	99%	0.0010
					Open	22%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
	Supply	[illegible]	[illegible]	[illegible]	Value change	29%		0.000					0.0000
		C109	YES	10.936	Short	57%	X	6.233	3.3V rail shorted to GND	SM2	CAN	99%	0.0623
					Open	32%		0.000					0.0000
					Value change	11%		0.000					0.0000
	Safety Monitor Cell 12	R174	YES	0.8108	Short	5%	X	0.041	Degraded EMC performance	SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C52	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D28	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 11	R173	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C49	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D27	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 10	R87	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C50	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D26	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 9	R77	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C47	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D24	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 8	R63	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C41	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D23	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 7	R121	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C69	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		[illegible]	[illegible]	[illegible]	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 6	R147	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C68	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D42	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 5	R133	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C64	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D46	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 4	R127	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C71	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D41	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 3	R117	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C67	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D45	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 2	R116	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C66	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D40	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
	Safety Monitor Cell 1	R118	YES	0.8108	Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162
					Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C65	YES	0.1455	Short	49%	X	0.071		SM8	6801 HW Monitr	60%	0.0285
					Open	22%	X	0.032		SM8	6801 HW Monitr	60%	0.0128
					Value change	29%	X	0.042		SM8	6801 HW Monitr	60%	0.0169
		D44	YES	0.72	Short	20%	X	0.144		SM8	6801 HW Monitr	60%	0.0576
					Open	45%	X	0.324		SM8	6801 HW Monitr	60%	0.1296
					Value change	35%		0.000					0.0000
		U5	YES	20.81	All	50%		0.000					0.0000
					All	25%		0.000					0.0000
					Short	5%	X	0.041		SM8	6801 HW Monitr	60%	0.0162

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
	Safety Monitor	R122	YES	0.8108	Open	59%	X	0.478		SM8	6801 HW Monitr	60%	0.1914
					Value change	36%		0.000					0.0000
		C73	YES	1.3233	Short	49%	X	0.648		SM8	6801 HW Monitr	60%	0.2594
					Open	22%	X	0.291		SM8	6801 HW Monitr	60%	0.1165
					Value change	29%	X	0.384		SM8	6801 HW Monitr	60%	0.1535
		C74	YES	0.5696	Short	49%	X	0.279		SM8	6801 HW Monitr	60%	0.1116
					Open	22%	X	0.125		SM8	6801 HW Monitr	60%	0.0501
					Value change	29%		0.000					0.0000
		C72	YES	0.5696	Short	49%	X	0.279		SM8	6801 HW Monitr	60%	0.1116
					Open	22%	X	0.125		SM8	6801 HW Monitr	60%	0.0501
					Value change	29%		0.000					0.0000
		R125	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R9	YES	2.3096	Short	5%		0.000					0.0000
					Open	59%	X	1.363					1.3626
					Value change	36%		0.000					0.0000
	Internal LTC temperature	C70	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C62	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R120	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R110	NO	0	Short	15%		0.000					0.0000
					Open	63%		0.000					0.0000
					Value change	22%		0.000					0.0000
	External LTC temperature	C78	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R160	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		J4-9	NO	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	Safety Line	D48	YES	1.2	Short	49%	X	0.588	Safety trip will oscillate	SM21	5kHz-STR	99%	0.0059
					Open	36%	X	0.432	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0043
					Value change	15%	X	0.180	safety trip unreliable, can't charge if <OA	SM21	5kHz-STR	99%	0.0018
		C75	YES	0.2009	Short	49%	X	0.098	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0010
					Open	22%	X	0.044	Safety trip will oscillate	SM21	5kHz-STR	99%	0.0004
					Value change	29%	X	0.058	safety trip unreliable, can't charge if <OA	SM21	5kHz-STR	99%	0.0006
		R123	YES	2.3096	Short	5%	X	0.115	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0012
					Open	59%	X	1.363	delayed safety trip, ctitcal on over V	SM21	5kHz-STR	99%	0.0136
					Value change	36%	X	0.831	safety trip unreliable, can't charge if <OA	SM21	5kHz-STR	99%	0.0083
		Q29	YES	1.2096	Short	51%	X	0.617	safety line satisfied all the time	SM21	5kHz-STR	99%	0.0062
					Open	5%	X	0.060	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0006
					Value change	17%	X	0.000	safety trip unreliable, can't charge if <OA	SM21	5kHz-STR	99%	0.0021
					Output low	22%	X	0.266	safety line satisfied all the time	SM21	5kHz-STR	99%	0.0027
					Output high	5%	X	0.060	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0006
		R126	YES	2.3096	Short	5%	X	0.115	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0012
					Open	59%	X	1.363	safety line satisfied all the time	SM21	5kHz-STR	99%	0.0136
					Value change	36%	X	0.831	safety trip unreliable, can't charge if <OA	SM21	5kHz-STR	99%	0.0083
		C139	YES	0.0744	Short	49%	X	0.036	safety line satisfied all the time	SM21	5kHz-STR	99%	0.0004
					Open	22%		0.000	no effect				0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	29%	X	0.022	increase in delay	SM21	5kHz-STR	99%	0.0002
		R124	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C140	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	Safety Relay	RLY1	YES	0.6612	Fails to trip	55%	X	0.364	safety line satisfied all the time	SM21	5kHz-STR	99%	0.0036
					Spurious trip	26%	X	0.172		SM21	5kHz-STR	99%	0.0000
					Short	19%	X	0.126		SM21	5kHz-STR	99%	0.0000
		R89	YES	0.7263	Short	5%	X	0.036		SM21	5kHz-STR	99%	0.0004
					Open	59%	X	0.428		SM21	5kHz-STR	99%	0.0043
					Value change	36%		0.000					0.0000
String Management Low Voltage	Power Supply	J3-1 PERM_SI_12V_B	NO	0	All	50%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge				0.0000
					All	50%		0.000					0.0000
		J1-20 0V	NO	0	All	50%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge or discharge				0.0000
					All	50%		0.000					0.0000
		U39	YES	10	All	50%	X	5.000	Power supply not stable may prevent SM from running correctly	SM24	PCc_PSU_Mon	90%	0.5000
					All	50%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge or discharge				0.0000
		C209	YES	0.5873	Short	49%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge				0.0000
					Open	22%	X	0.129	Reduced EMC performance	SM24	PCc_PSU_Mon	90%	0.0000
					Value change	29%		0.000					0.0000
		D56	YES	4.4928	Short	20%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge or discharge				0.0000
					Open	45%	X	2.022	Reduced EMC performance	SM24	PCc_PSU_Mon	90%	0.2022
					Value change	35%		0.000					0.0000
		R227		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R229		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		D58		0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		Q18		0	Short	73%		0.000					0.0000
					Open	27%		0.000					0.0000
		R228		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		D29		0	Short	20%		0.000					0.0000
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		D57		0	Short	20%		0.000					0.0000
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		Q17		0	Short	51%		0.000					0.0000
					Open	5%		0.000					0.0000
					Value change	17%		0.000					0.0000
					Output low	22%		0.000					0.0000
					Output high	5%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
		R231		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C212		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C208	YES	0.2009	Short	49%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge or discharge				0.0000
					Open	22%	X	0.044	Reduced EMC performance	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		L9	YES	0.0216	Short	42%	X	0.009	Reduced EMC performance	SM24	PCc_PSU_Mon	90%	0.0009
					open	42%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge or discharge				0.0000
					Value change	16%		0.000					0.0000
		C210	YES	0.2009	Short	49%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge or discharge				0.0000
					Open	22%	X	0.044	Reduced EMC performance	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C211	YES	0.0645	Short	49%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge or discharge				0.0000
					Open	22%	X	0.014	Power supply not stable may prevent SM from running correctly	SM24	PCc_PSU_Mon	90%	0.0014
					Value change	29%		0.000					0.0000
		C174	YES	0.0645	Short	49%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge or discharge				0.0000
					Open	22%	X	0.014	Power supply not stable may prevent SM from running correctly	SM24	PCc_PSU_Mon	90%	0.0014
					Value change	29%		0.000					0.0000
		C175	YES	0.0645	Short	49%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge or discharge but can self discharge				0.0000
					Open	22%	X	0.014	Power supply not stable may prevent SM from running correctly	SM24	PCc_PSU_Mon	90%	0.0014
					Value change	29%		0.000					0.0000
		R103	YES	2.3096	Short	5%		0.000	If SM is not powered the contactors cannot pull in so cannot over charge or discharge but can self discharge				0.0000
					Open	59%	X	1.363	SM may power up due to noise but digital inputs are monitored, if not stable will power down again	SM15	PCc ADref	99%	0.0136
					Value change	36%		0.000					0.0000
		U40	NO	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		R230	YES	0.7785	Short	5%	X	0.039	Reduced EMC performance	SM24	PCc_PSU_Mon	90%	0.0039
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R232	YES	0.7785	Short	5%	X	0.039	Reduced EMC performance	SM24	PCc_PSU_Mon	90%	0.0039
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R233	YES	0.7785	Short	5%	X	0.039	Reduced EMC performance	SM24	PCc_PSU_Mon	90%	0.0039
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R14	YES	0.8108	Short	5%	X	0.041	Reduced EMC performance	SM24	PCc_PSU_Mon	90%	0.0041
					Open	59%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	36%		0.000					0.0000
		C213		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R234	YES	0.7195	Short	5%		0.000					0.0000
					Open	59%	X	0.424	No Clean power up reset provided to TMS570	SM16	Q&A Wdog	99%	0.0042
					Value change	36%		0.000					0.0000
		R235	No	0	Short	5%		0.000					0.0000
					Open	59%		0.000	No Powewr seuuply analogue monitoring at TMS570				0.0000
					Value change	36%		0.000					0.0000
		C215	No	0	Short	49%		0.000	No Powewr seuuply analogue monitoring at TMS570				0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R328	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000	Device Stays in reset state. If SM is not running the contactors cannot pull in so cannot over charge				0.0000
					Value change	36%		0.000					0.0000
		R240	NO	0	Short	5%		0.000	Not Used in Q&A mode				0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R104	NO	0	Short	5%		0.000	CAN Wake Up Input to PSU not used in this application				0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R106	NO	0	Short	5%		0.000	CAN Wake up function will not work				0.0000
					Open	59%		0.000	CAN wake up input may float high and Wake up PSU				0.0000
					Value change	36%		0.000					0.0000
		C219	Yes	0.5873	Short	49%	x	0.288	+6V supply feedback will be zero	SM24	PCc_PSU_Mon	90%	0.0288
					Open	22%	x	0.129	Noise may affect +6V supply	SM24	PCc_PSU_Mon	90%	0.0129
					Value change	29%		0.000					0.0000
		L10	YES	0.0017	Short	42%	X	0.001	+6V supply incorrect operation	SM24	PCc_PSU_Mon	90%	0.0001
					Open	42%	X	0.001	+6V supply incorrect operation	SM24	PCc_PSU_Mon	90%	0.0001
					Value change	16%	X	0.000	+6V supply incorrect operation	SM24	PCc_PSU_Mon	90%	0.0000
		D59	YES	1.6542	Short	49%	X	0.811	+6V supply incorrect operation	SM24	PCc_PSU_Mon	90%	0.0811
					Open	36%	X	0.596	+6V supply incorrect operation	SM24	PCc_PSU_Mon	90%	0.0596
					Value change	15%	X	0.248	+6V supply incorrect operation	SM24	PCc_PSU_Mon	90%	0.0248
		C16		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R284		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C214		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		Q19		0	Short	51%							0.0000
					Open	5%							0.0000
					Value change	17%							0.0000
					Output High	22%							0.0000
					Output low	5%							0.0000
		R236		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	36%		0.000					0.0000
		R237		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R239		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C216		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C217	Yes	0.7269	Short	49%	X	0.356	+3.3V supply will be shorted to ground	SM24	PCc_PSU_Mon	90%	0.0356
					Open	22%	X	0.160	+3.3v supply will be noisy	SM24	PCc_PSU_Mon	90%	0.0160
					Value change	29%		0.000	+3.3v supply may be noisy				0.0000
		C218	Yes	1.6809	Short	49%	X	0.824	+5V supply will be shorted to ground	SM24	PCc_PSU_Mon	90%	0.0824
					Open	22%	X	0.370	+5V supply will be noisy	SM24	PCc_PSU_Mon	90%	0.0370
					Value change	29%		0.000	+5V supply may be noisy				0.0000
		C206	Yes	0.2009	Short	49%	X	0.098	+5V ADC supply will be shorted to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	+5V ADC supply will be noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000	+5V ADC supply may be noisy				0.0000
		C220	No	0	Short	49%		0.000	Sensor Supply sense input will be at ground level affecting SENSOR_SO_5V_B	SM16	Q&A Wdog	99%	0.0000
					Open	22%		0.000	SENSOR_SO_5V_B Will be noisy				0.0000
					Value change	29%		0.000					0.0000
		C97	No	0	Short	49%		0.000	Sensor Supply sense input will be at ground level affecting SENSOR_SO_5V_B				0.0000
					Open	22%		0.000	SENSOR_SO_5V_B will be noisy				0.0000
					Value change	29%		0.000					0.0000
	Microcontroller and associated decoupling	U8	Yes	1.47	All	50%	X	0.735	Incorrect operation of overvolateg detection and opening of contactors	SM16	Q&A Wdog	99%	0.0074
					All	50%		0.000					0.0000
		C53	Yes	0.2009	Short	49%	X	0.098	VccIO (3V3) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	VccIO (3V3) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C54	YES	0.2009	Short	49%	X	0.098	Vcc (1.2Vu) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	Vcc (1.2Vu) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C55	YES	0.2009	Short	49%	X	0.098	VccIO (3V3) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	VccIO (3V3) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C56	YES	0.2009	Short	49%	X	0.098	Vcc (1.2Vu) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	Vcc (1.2Vu) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C50	YES	0.2009	Short	49%	X	0.098	VccIO (3V3) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	VccIO (3V3) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C47	YES	0.2009	Short	49%	X	0.098	Vcc (1.2Vu) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	Vcc (1.2Vu) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C46	YES	0.2009	Short	49%	X	0.098	Vcc (1.2Vu) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	Vcc (1.2Vu) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C44	YES	0.2009	Short	49%	X	0.098	Vcc (1.2Vu) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	Vcc (1.2Vu) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
		C42	YES	0.2009	Short	49%	X	0.098	ADREFHI (+5V ADC REF) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	ADREFHI (+5V ADC REF) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C40	YES	0.5696	Short	49%	X	0.279	VCCAD (+5V) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0279
					Open	22%	X	0.125	VCCAD (+5V)| ADC REF|Noisy	SM24	PCc_PSU_Mon	90%	0.0125
					Value change	29%		0.000					0.0000
		L3	YES	0.3828	Short	42%	X	0.161	VCCAD (+5V)| ADC REF|Noisy	SM24	PCc_PSU_Mon	90%	0.0161
					Open	42%	X	0.161	VCCAD (+5V) not powered	SM24	PCc_PSU_Mon	90%	0.0161
					Value change	16%		0.000					0.0000
		C248	YES	0.2009	Short	49%	X	0.098	VCCAD (+5V) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	VCCAD (+5V)| ADC REF|Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C36	YES	0.2009	Short	49%	X	0.098	Vcc (1.2Vu) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	Vcc (1.2Vu) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C35	YES	0.2009	Short	49%	X	0.098	Vcc (1.2Vu) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	Vcc (1.2Vu) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C34	YES	0.2009	Short	49%	X	0.098	VccIO (3V3) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	VccIO (3V3) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C41	YES	0.2009	Short	49%	X	0.098	Vcc (1.2Vu) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	Vcc (1.2Vu) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C43	YES	0.2009	Short	49%	X	0.098	VccIO (3V3) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	VccIO (3V3) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C45	YES	0.2009	Short	49%	X	0.098	Vcc (1.2Vu) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	Vcc (1.2Vu) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C48	YES	0.2009	Short	49%	X	0.098	VccIO (3V3) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	VccIO (3V3) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C49	YES	0.2009	Short	49%	X	0.098	VccIO (3V3) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	VccIO (3V3) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
		C51	YES	0.2009	Short	49%	X	0.098	Vcc (1.2Vu) pulled to ground	SM24	PCc_PSU_Mon	90%	0.0098
					Open	22%	X	0.044	Vcc (1.2Vu) Noisy	SM24	PCc_PSU_Mon	90%	0.0044
					Value change	29%		0.000					0.0000
	Micro Oscillator	X1	NO	0	Open	89%		0.000	TMS570 Not running so outputs off so cannot close contcators				0.0000
					No Oscillation	11%		0.000					0.0000
		R44	YES	0.8564	Short	5%		0.000	TMS570 Not running so outputs off so cannot close contcators				0.0000
					Open	59%		0.000	TMS570 Not running so outputs off so cannot close contcators				0.0000
					Value change	36%	X	0.308	May run at incorrect frequency	SM16	Q&A Wdog	99%	0.0031
		R45	YES	0.7722	Short	5%		0.000					0.0000
					Open	59%		0.000	TMS570 Not running so outputs off so cannot close contcators				0.0000
					Value change	36%	X	0.278	May run at incorrect frequency	SM16	Q&A Wdog	99%	0.0028
		C57	YES	0.0585	Short	49%		0.000	TMS570 Not running so outputs off so cannot close contcators				0.0000
					Open	22%		0.000	TMS570 Not running so outputs off so cannot close contcators				0.0000
					Value change	29%	X	0.017	May run at incorrect frequency	SM16	Q&A Wdog	99%	0.0002
					Short	49%		0.000	TMS570 Not running so outputs off so cannot close contcators				0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
		C59	YES	0.0585	Open	22%		0.000	TMS570 Not running so outputs off so cannot close contcators				0.0000
					Value change	29%	X	0.017	May run at incorrect frequency	SM16	Q&A Wdog	99%	0.0002
	Micro ADC reference	U7	NO	0	Open	20%		0.000	No ADC (+5V-ADC-REF)				0.0000
					Short	45%		0.000	No ADC (+5V-ADC-REF)				0.0000
					Value Change	35%		0.000	Incorrect ADC Reference				0.0000
		D61	NO	0	Short	49%		0.000	Input Voltage to U7 >5.5V, but not above abs max rating				0.0000
					Open	36%		0.000	No Input Voltage to U7 so no ADC reference				0.0000
					Value change	15%		0.000	ADC ref may not control correctly				0.0000
		C37	NO	0	Short	49%		0.000	No ADC (+5V-ADC-REF)				0.0000
					Open	22%		0.000	ADC Vref will be noisy				0.0000
					Value change	29%		0.000	ADC Vref may be noisy				0.0000
		C39	NO	0	Short	49%		0.000	No ADC (+5V-ADC-REF)				0.0000
					Open	22%		0.000	ADC Vref will be noisy				0.0000
					Value change	29%		0.000	ADC Vref may be noisy				0.0000
	Jtag	J7-1	YES	0.05	All	50%	X	0.025	TMS570 May not run correctly	SM16	Q&A Wdog	99%	0.0003
					All	50%		0.000					0.0000
		J7-2	YES	0.05	All	50%	X	0.025	TMS570 May not run correctly	SM16	Q&A Wdog	99%	0.0003
					All	50%		0.000					0.0000
		J7-3	YES	0.05	All	50%	X	0.025	TMS570 May not run correctly	SM16	Q&A Wdog	99%	0.0003
					All	50%		0.000					0.0000
		J7-4	YES	0.05	All	50%	X	0.025	TMS570 May not run correctly	SM16	Q&A Wdog	99%	0.0003
					All	50%		0.000					0.0000
		J7-5	YES	0.05	All	50%	X	0.025	TMS570 May not run correctly	SM16	Q&A Wdog	99%	0.0003
					All	50%		0.000					0.0000
		J7-6	YES	0.05	All	50%	X	0.025	TMS570 May not run correctly	SM16	Q&A Wdog	99%	0.0003
					All	50%		0.000					0.0000
	Battery CAN	C222	YES	0.0618	Short	49%	X	0.030	CAN-H shorted to GND	SM2	CAN	99%	0.0003
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R241	YES	0.7629	Short	5%	X	0.038	CAN Hi - Lo Bias incorrect	SM2	CAN	99%	0.0004
					Open	59%	X	0.450	CAN Hi - Lo Bias incorrect	SM2	CAN	99%	0.0045
					Value change	36%	X	0.275	CAN Hi - Lo Bias incorrect	SM2	CAN	99%	0.0027
		R242	YES	0.7629	Short	5%	X	0.038	CAN Hi - Lo Bias incorrect	SM2	CAN	99%	0.0004
					Open	59%	X	0.450	CAN Hi - Lo Bias incorrect	SM2	CAN	99%	0.0045
					Value change	36%	X	0.275	CAN Hi - Lo Bias incorrect	SM2	CAN	99%	0.0027
		D60	YES	2.34	Short	20%	X	0.468	CAN-H shorted to GND	SM2	CAN	99%	0.0047
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		C223	YES	0.0618	Short	49%	X	0.030	CAN-L shorted to GND	SM2	CAN	99%	0.0003
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C224	YES	0.1455	Short	49%	X	0.071	CAN Hi - Lo Bias incorrect				0.0713
					Open	22%	X	0.032	CAN Hi - Lo Bias incorrect				0.0320
					Value change	29%	X	0.042	CAN Hi - Lo Bias incorrect				0.0422
		L11	YES	0.0331	Short	42%	X	0.014	CAN does not function	SM2	CAN	99%	0.0001
					Open	42%	X	0.014	CAN does not function	SM2			0.0139
					Value change	16%		0.000					0.0000
		U41	YES	1	All	50%	X	0.500	CAN does not function	SM2	CAN	99%	0.0050
					All	50%		0.000	Failures do not violate safety goal				0.0000
		C221	YES	0.489	Short	49%	X	0.240	+5V supply shorted to ground	SM2	CAN	99%	0.0024
					Open	22%		0.000	Can May become unreliable				0.0000
					Value change	29%		0.000					0.0000
		J1-22	YES	0.05	All	50%	X	0.025	BATT_OUT_CN_LO_B fault	SM2	CAN	99%	0.0003
					All	50%		0.000					0.0000
		J1-23	YES	0.05	All	50%	X	0.025	BATT_OUT_CN_HI_B fault	SM2	CAN	99%	0.0003
					All	50%		0.000					0.0000
		J1-25	YES	0.05	All	50%	X	0.025	BATT_IN_CN_HI_B fault	SM2	CAN	99%	0.0003
					All	50%		0.000					0.0000
		J1-26	YES	0.05	All	50%	X	0.025	BATT_IN_CN_LO_B fault	SM2	CAN	99%	0.0003

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					All	50%		0.000					0.0000
		J6-1	YES	0.0081	All	50%	X	0.004	BATT_OUT_CN_LO_B fault	SM2	CAN	99%	0.0000
					All	50%		0.000					0.0000
		J6-5	YES	0.0081	All	50%	X	0.004	BATT_OUT_CN_HI_B fault	SM2	CAN	99%	0.0000
					All	50%		0.000					0.0000
	Vehicle CAN	C11	no	0	Short	49%	X	0.000	CAN-H shorted to GND	SM17	Vehicle CAN Checks	90%	0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R3	no	0	Short	5%	X	0.000	CAN Hi - Lo Bias incorrect	SM17	Vehicle CAN Checks	90%	0.0000
					Open	59%	X	0.000	CAN Hi - Lo Bias incorrect	SM17	Vehicle CAN Checks	90%	0.0000
					Value change	36%	X	0.000	CAN Hi - Lo Bias incorrect	SM17	Vehicle CAN Checks	90%	0.0000
		R4	no	0	Short	5%	X	0.000	CAN Hi - Lo Bias incorrect	SM17	Vehicle CAN Checks	90%	0.0000
					Open	59%	X	0.000	CAN Hi - Lo Bias incorrect	SM17	Vehicle CAN Checks	90%	0.0000
					Value change	36%	X	0.000	CAN Hi - Lo Bias incorrect	SM17	Vehicle CAN Checks	90%	0.0000
		D3	no	0	Short	20%	X	0.000	CAN-H shorted to GND	SM17	Vehicle CAN Checks	90%	0.0000
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		C12	no	0	Short	49%	X	0.000	CAN-L shorted to GND	SM17	Vehicle CAN Checks	90%	0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C13	no	0	Short	49%	X	0.000	CAN Hi - Lo Bias incorrect	SM17	Vehicle CAN Checks	90%	0.0000
					Open	22%	X	0.000	CAN Hi - Lo Bias incorrect	SM17	Vehicle CAN Checks	90%	0.0000
					Value change	29%	X	0.000	CAN Hi - Lo Bias incorrect	SM17	Vehicle CAN Checks	90%	0.0000
		L2	no	0	Short	42%	X	0.000	CAN does not function	SM17	Vehicle CAN Checks	90%	0.0000
					Open	42%	X	0.000	CAN does not function	SM17			0.0000
					Value change	16%		0.000					0.0000
		U2	no	0	All	50%	X	0.000	CAN does not function	SM17	Vehicle CAN Checks	90%	0.0000
					All	50%		0.000	Failures do not violate safety goal				0.0000
		C9	no	0	Short	49%	X	0.000	+12V shorted to gnd - CAN will not function	SM17	Vehicle CAN Checks	90%	0.0000
					Open	22%	X	0.000	Noise on Can Transmissions	SM17	Vehicle CAN Checks	90%	0.0000
					Value change	29%		0.000	Possible noise on CAN				0.0000
		R5	no	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q1	no	0	Short	73%		0.000					0.0000
					Open	27%		0.000					0.0000
		C5	no	0	Short	49%	X	0.000	+5V shorted to gnd - CAN will not function	SM17	Vehicle CAN Checks	90%	0.0000
					Open	22%	X	0.000	Noise on Can Transmissions	SM17	Vehicle CAN Checks	90%	0.0000
					Value change	29%		0.000	Possible noise on CAN				0.0000
		C6	no	0	Short	49%	X	0.000	VI/O shorted to gnd - CAN will not function	SM17	Vehicle CAN Checks	90%	0.0000
					Open	22%	X	0.000	Noise on Can Transmissions	SM17	Vehicle CAN Checks	90%	0.0000
					Value change	29%		0.000	Possible noise on CAN				0.0000
		J1-11	no	0	All	50%	X	0.000	VEH_CN_HI_B fault	SM17	Vehicle CAN Checks	90%	0.0000
					All	50%		0.000					0.0000
		J1-12	no	0	All	50%	X	0.000	VEH_CN_LO_B_fault	SM17	Vehicle CAN Checks	90%	0.0000
					All	50%		0.000					0.0000
		SCIRX Pin 38	no		All	50%		0.000					
	LV_RX_DI_UC	SCITX Pin 39	no	0	All	50%		0.000					
	LV_TX_DO_UC	J1-29		0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	DISCHG_REQ_DI_V_B	C93		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R93		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
					Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	36%		0.000					0.0000
		R92		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R95		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		D20		0	Short	20%		0.000					0.0000
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		C92		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		J1-30		0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	CHG_REQ_DI_V_B	C95		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R97		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R98		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R96		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R99		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		D21		0	Short	20%		0.000					0.0000
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		C94		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		Q11		0	Short	73%		0.000					0.0000
					Open	27%		0.000					
	SW-SO_12V_I1, 12V enable from Micro	R201		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R199		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		D39		0	Short	20%		0.000					0.0000
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		Q10		0	Short	51%		0.000					0.0000
					Open	5%		0.000					0.0000
					Value change	17%		0.000					0.0000
					Output High	22%		0.000					0.0000
					Output low	5%		0.000					0.0000
		R202		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	SW_SO_12V_AI_V_				Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
	UC, 12V sense to micro				Value change	36%		0.000					0.0000
		C187		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D40		0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C186		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		J6-2		0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	CMB_SO_8V0_B	J6-7	Yes	0.0081	All	50%	X	0.004	No output to cell monitor board	SM2	CAN	99%	0.0000
					All	50%		0.000					0.0000
		C256	Yes	0.2929	Short	49%		0.000	No output to cell monitor board				0.0000
					Open	22%	X	0.064	Reduced EMC performance	SM21	5kHz-STR	99%	0.0006
					Value change	29%		0.000					0.0000
		L8	Yes	0.0004	Short	42%	X	0.000	Reduced EMC performance	SM21	5kHz-STR	99%	0.0000
					Open	42%		0.000	No output to cell monitor board				0.0000
					Value change	16%		0.000					0.0000
		C193	Yes	0.3177	Short	49%		0.000	No output to cell monitor board				0.0000
					Open	22%	X	0.070	Reduced EMC performance	SM21	5kHz-STR	99%	0.0007
					Value change	29%		0.000					0.0000
		C194	Yes	0.3177	Short	49%		0.000	No output to cell monitor board				0.0000
					Open	22%	X	0.070	Reduced EMC performance	SM21	5kHz-STR	99%	0.0007
					Value change	29%		0.000					0.0000
		C195	Yes	0.3177	Short	49%		0.000	No output to cell monitor board				0.0000
					Open	22%	X	0.070	Reduced EMC performance	SM21	5kHz-STR	99%	0.0007
					Value change	29%		0.000					0.0000
		C196	Yes	0.3177	Short	49%		0.000	No output to cell monitor board				0.0000
					Open	22%	X	0.070	Reduced EMC performance	SM21	5kHz-STR	99%	0.0007
					Value change	29%		0.000					0.0000
		U32	Yes	0.6	All	50%	x	0.300	Power not stable	SM14	PCc ADref	99%	0.0030
					All	50%		0.000					0.0000
		R208	Yes	0.7895	Short	5%		0.000	No output to cell monitor board				0.0000
					Open	59%		0.000	U32 expects synchronisation input so no output				0.0000
					Value change	36%	X	0.284	Variation in switching frequency, may affect cell monitor board	SM21	5kHz-STR	99%	0.0028
		R209	Yes	0.7177	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%	X	0.258	Incorrect compensation	SM14	PCc ADref	99%	0.0026
		C254	Yes	0.1454	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%	X	0.042	Incorrect compensation	SM14	PCc ADref	99%	0.0004
		C197	Yes	0.1467	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%	X	0.043	Incorrect compensation	SM14	PCc ADref	99%	0.0004
		D38	Yes	0.197	Short	20%		0.000					0.0000
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		L7	Yes	0.0011	Short	42%	X	0.000	Incorrect Volatge output	SM14	PCc ADref	99%	0.0000
					Open	42%		0.000	No output to cell monitor board				0.0000
					Value change	16%	X	0.000	Reduced EMC performance	SM21			0.0002
		C190	Yes	0.8617	Short	49%		0.000	No output to cell monitor board				0.0000
					Open	22%	X	0.190	Incorrect Volatge output	SM14	PCc ADref	99%	0.0019
					Value change	29%		0.000					0.0000
		C191	Yes	0.8617	Short	49%		0.000	No output to cell monitor board				0.0000
					Open	22%	X	0.190	Incorrect Volatge output	SM14	PCc ADref	99%	0.0019
					Value change	29%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Short	49%		0.000	No output to cell monitor board				0.0000
		C192	Yes	0.8617	Open	22%	X	0.190	Incorrect Voltage output	SM14	PCc ADref	99%	0.0019
					Value change	29%		0.000					0.0000
					Short	5%		0.000					0.0000
		R13	Yes	0.8556	Open	59%		0.000					0.0000
					Value change	36%	X	0.308	Incorrect Voltage output	SM14	PCc ADref	99%	0.0031
					Short	5%		0.000					0.0000
		R210	Yes	0.7319	Open	59%		0.000					0.0000
					Value change	36%	X	0.263	Incorrect Voltage output	SM14	PCc ADref	99%	0.0026
	CBM_SO_8V0_EN_DO_UC, enable from micro	Q27	Yes	0.0746	Short	73%	X	0.054	cell monitor board always on, drain power	SM14	PCc ADref	99%	0.0005
					Open	27%		0.000	No output to cell monitor board				0.0000
					Short	5%		0.000					0.0000
		R273	No	0	Open	59%		0.000	No output to cell monitor board				0.0000
					Value change	36%		0.000					0.0000
					Short	20%		0.000	No output to cell monitor board				0.0000
		D25	No	0	Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
					Short	5%		0.000	No output to cell monitor board				0.0000
		R274	No	0	Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
					Short	51%	X	0.617	cell monitor board always on, drain power	SM14	PCc ADref	99%	0.0062
					Open	5%		0.000					0.0000
		Q28	Yes	1.2096	Value change	17%		0.000					0.0000
					Output High	22%		0.000					0.0000
					Output low	5%		0.000					0.0000
					Short	49%		0.000					0.0000
		C198	No	0	Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
					Short	5%		0.000					0.0000
		R207	No	0	Open	59%		0.000	No output to cell monitor board				0.0000
					Value change	36%		0.000					0.0000
					Short	5%		0.000	No output to cell monitor board				0.0000
		R285	No	0	Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	CBM_SO_8V0_AI_V_UC, 8V0 feedback to micro	R100	Yes	0.7785	Short	5%	X	0.039	Incorrect Voltage detection	SM14	PCc ADref	99%	0.0004
					Open	59%	X	0.459	Incorrect Voltage detection	SM14	PCc ADref	99%	0.0046
					Value change	36%	X	0.280	Incorrect Voltage detection	SM14	PCc ADref	99%	0.0028
					Short	5%	X	0.039	Incorrect Voltage detection	SM14	PCc ADref	99%	0.0004
		R101	Yes	0.7785	Open	59%	X	0.459	Incorrect Voltage detection	SM14	PCc ADref	99%	0.0000
					Value change	36%	X	0.280	Incorrect Voltage detection	SM14	PCc ADref	99%	0.0000
					Short	49%	X	0.098	Incorrect Voltage detection	SM14	PCc ADref	99%	0.0010
		C96	Yes	0.2009	Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	SAFETY_OUT_AO_V_V	R171	Yes	0.7355	Short	5%	X	0.037	Safety trips, can't charge if <0A	SM21	5kHz-STR	99%	0.0004
					Open	59%	X	0.434	Safety trips, can't charge if <0A	SM21	5kHz-STR	99%	0.0043
					Value change	36%	X	0.265	Safety trips, can't charge if <0A	SM21	5kHz-STR	99%	0.0026
	SAFETY_IN_AI_V_B	R176	Yes	0.7355	Short	5%	X	0.037	Safety trips, can't charge if <0A	SM21	5kHz-STR	99%	0.0004
					Open	59%	X	0.434	Safety trips, can't charge if <0A	SM21	5kHz-STR	99%	0.0043
					Value change	36%	X	0.265	Safety trips, can't charge if <0A	SM21	5kHz-STR	99%	0.0026
					Short	5%	X	0.039	Safety trips, can't charge if <0A	SM21	5kHz-STR	99%	0.0004
		R283	Yes	0.7785	Open	59%	X	0.459	Safety trips, can't charge if <0A	SM21	5kHz-STR	99%	0.0046

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	36%	X	0.280	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0028
		C246	Yes	0.2009	Short	49%	X	0.098	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0010
					Open	22%	X	0.044	Reduced EMC performance	SM21	5kHz-STR	99%	0.0004
					Value change	29%		0.000	no effect				0.0000
		C247	Yes	0.0764	Short	49%	X	0.037	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0004
					Open	22%	X	0.017	Reduced EMC performance	SM21	5kHz-STR	99%	0.0002
					Value change	29%		0.000	no effect				0.0000
		D26	Yes	1.4811	Short	49%	X	0.726	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0073
					Open	36%	X	0.533	Reduced EMC performance	SM21	5kHz-STR	99%	0.0053
					Value change	15%		0.000	no effect				0.0000
		R173	Yes	0.8108	Short	5%	X	0.041	Window higher V, Safety trips, can't chg if <OA	SM21	5kHz-STR	99%	0.0004
					Open	59%	X	0.478	Window lower V, Safety trips, can't chg if <OA	SM21	5kHz-STR	99%	0.0048
					Value change	36%	X	0.292	Window incorrect V, Safety trips, can't chg if <OA	SM21	5kHz-STR	99%	0.0029
		R178	Yes	0.7314	Short	5%	X	0.037	Reduced window,Safety trips, can't chg if <OA	SM21	5kHz-STR	99%	0.0004
					Open	59%	X	0.432	Wide window, cant trip, overcharge if >OA	SM21	5kHz-STR	99%	0.0043
					Value change	36%	X	0.263	incorrect window - indeterminate	SM21	5kHz-STR	99%	0.0026
		R181	Yes	0.7319	Short	5%	X	0.037	Wide window, cant trip, overcharge if >OA	SM21	5kHz-STR	99%	0.0004
					Open	59%	X	0.432	Reduced window,Safety trips, can't chg if <OA	SM21	5kHz-STR	99%	0.0043
					Value change	36%	X	0.263	Window incorrect V, Safety trips, can't chg if <OA	SM21	5kHz-STR	99%	0.0026
		U25	Yes	1	All	50%	X	0.500	incorrect window - indeterminate	SM21	5kHz-STR	99%	0.0050
					All	50%		0.000					0.0000
		R174	Yes	0.8919	Short	5%	X	0.045	safety line satisfied all the time	SM21	5kHz-STR	99%	0.0004
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R175	Yes	0.8919	Short	5%	X	0.045	Safety trips, can't charge if <OA	SM21	5kHz-STR	99%	0.0004
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R180	Yes	0.8108	Short	5%		0.000					0.0000
					Open	59%	X	0.478	Safety trip will oscillate	SM21	5kHz-STR	99%	0.0048
					Value change	36%		0.000					0.0000
		C157		0	Short	49%		0.000	safety line satisfied all the time	SM21	5kHz-STR	99%	0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R177		0	Short	5%		0.000	safety line satisfied all the time	SM21	5kHz-STR	99%	0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	SAFETY_OK_DLY_DI_V_UC	C156		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R179		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	SAFETY_OK_DI_V_UC	D33		0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		R172		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C155		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		[illegible]		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	36%		0.000					0.0000
	SAFETY_IN_AI_V_UC	R170		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C151		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D32		0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C152		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		Q2		0	Short	73%		0.000					0.0000
					Open	27%		0.000					0.0000
	HVIL_END_DO_UC	R10		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		U3		0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		R18		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	HVIL_OUT_SW_AO_V_B	D7		0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		R23		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C24		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C22		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	HVIL_OUT_AI_A_UC	U4		0	All	50%		0.000					0.0000
					All	50%		0.000					
		C17		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R17		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C20		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R11		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	HVIL_OUT_SW_AO_V_B	R12		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C14		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D4		0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
					Short	49%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
		C15		0	Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		J1-1		0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	HVIL_OUT_SW_AO_	J1-17		0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	HVIL_OUT_RES_AO_	J1-2		0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	HVIL_IN_AI_V_B	R26		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R31		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	HVIL_IN_AI_A_C	R30		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C28		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D9		0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C29		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R27		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C27		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R20		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	HVIL_OK_DI_V_UC	R25		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R32		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		U5		0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		R21		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C23		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R24		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		D8		0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		R19		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		[illegible]		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	29%		0.000					0.0000
		R22		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	HVIL_OK_DLY_DI_V_UC	R29		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C30		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R28		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C31		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R15		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	HVIL_IN_SW_AO_V_B	R16		0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C18		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D5		0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C19		0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		TMS570 N2HET1[16]		0	All	50%		0.000					
					All	50%		0.000					
	HVPOS1_EN_DO_UC	R289	YES	0.7195	Short	5%		0.000					0.0000
					Open	59%		0.000	Can't enable HVPOS1_P_DO_V_B				0.0000
					Value change	36%		0.000					0.0000
		U22	X	0	All	50%			Output high would enable HVPOS1_P_DO_V_B				0.0000
					All	50%							0.0000
		R219	YES	0.8557	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q14	YES	1.2096	Short	51%	X	0.617	HVPOS1_P_DO_V_B permanently enabled	SM23	PCc_POSCON	99%	0.0062
					Open	5%		0.000					0.0000
					Value change	17%		0.000					0.0000
					Output High	22%		0.000					0.0000
					Output low	5%	X	0.060	HVPOS1_P_DO_V_B permanently enabled	SM23	PCc_POSCON	99%	0.0006
		R217	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		D43	NO	0	Short	49%		0.000					0.0000
					Open	36%		0.000	Reduced EMC performance				0.0000
					Value change	15%		0.000					0.0000
		D44	NO	0	Short	49%		0.000					0.0000
					Open	36%		0.000	Reduced EMC Performance				0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	15%		0.000					0.0000
		C147	NO	0	Short	49%		0.000					0.0000
					Open	22%		0.000	Reduced EMC Performance				0.0000
					Value change	29%		0.000					0.0000
		D41	NO	0	Short	20%		0.000					0.0000
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		R215	NO	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q12	YES	1.2096	Short	51%	X	0.617	HVPOS1_P_DO_V_B permanently enables	SM23	PCc_POSCON	99%	0.0062
					Open	5%		0.000					0.0000
					Value change	17%		0.000					0.0000
					Output High	22%	X	0.266	HVPOS1_P_DO_V_B permanently enables	SM23	PCc_POSCON	99%	0.0027
					Output low	5%		0.000					0.0000
		J3-4	NO	0	All	50%		0.000					
					All	50%		0.000					
	HVPOS1_AI_A_UC	TMS570 ADIN[19] pin 63	NO	0	All	50%		0.000	HVPOS1_P_AI_A_UC cannot measure current in HVPOS1_P_DO_V_B				0.0000
					All	50%		0.000					
	HVPOS1_P_AI_A_UC	R211	NO	0	Short	5%		0.000	HVPOS1_P_AI_A_UC cannot measure current in HVPOS1_P_DO_V_B				0.0000
					Open	59%		0.000	HVPOS1_P_DO_V_B cannot turn on				0.0000
					Value change	36%		0.000	HVPOS1_P_AI_A_UC measures incorrect current in HVPOS1_P_DO_V_B				0.0000
		U33	NO	0	All	50%		0.000	HVPOS1_P_AI_A_UC measures incorrect current in HVPOS1_P_DO_V_B				0.0000
					All	50%		0.000					
		C104	NO	0	Short	49%		0.000	+12V shorted to ground				0.0000
					Open	22%		0.000	Reduced decoupling on +12V supply				0.0000
					Value change	29%		0.000					0.0000
		C98	NO	0	Short	49%		0.000	+5V shorted to ground				0.0000
					Open	22%		0.000	Reduced decoupling on +5V supply				0.0000
					Value change	29%		0.000					0.0000
		R213	NO	0	Short	5%		0.000	HVPOS1_P_AI_A_UC measures incorrect current in HVPOS1_P_DO_V_B				0.0000
					Open	59%		0.000	HVPOS1_P_AI_A_UC measures incorrect current in HVPOS1_P_DO_V_B				0.0000
					Value change	36%		0.000	HVPOS1_P_AI_A_UC measures incorrect current in HVPOS1_P_DO_V_B				0.0000
		C199	NO	0	Short	49%		0.000	HVPOS1_P_AI_A_UC measures incorrect current in				0.0000
					Open	22%		0.000	HVPOS1_P_AI_A_UC measures incorrect current in HVPOS1_P_DO_V_B				0.0000
					Value change	29%		0.000	HVPOS1_P_AI_A_UC measures incorrect current in HVPOS1_P_DO_V_B				0.0000
	HVPOS1_N_DO_V_B	J3-12	YES	0.05	All	50%	X	0.025	incorrect drive to contactor	SM23	PCc_POSCON	99%	0.0003
					All	50%		0.000					0.0000
		R36	YES	0.8108	Short	5%		0.000					0.0000
					Open	59%	X	0.478	trips contactor, prevents charge	SM23	PCc_POSCON	99%	0.0048
					Value change	36%		0.000					0.0000
		U36	YES	10	All	50%	X	5.000	trips contactor, prevents charge or continually discharges	SM23	PCc_POSCON	99%	0.0500
					All	50%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
		D49	YES	0.7879	Short	20%	X	0.158	Prevents contacor closing	SM23	PCc_POSCON	99%	0.0016
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		C150	YES	0.5873	Short	49%	X	0.288	transient closure of contactor	SM23	PCc_POSCON	99%	0.0029
					Open	22%	X	0.129	Noise increase, emc performance	SM23	PCc_POSCON	99%	0.0013
					Value change	29%		0.000					0.0000
		J3-6	YES	0.05	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	HVNEG_P_DO_V_B	R221	YES	0.8919	Short	5%	X	0.045	Prevents contactor closure, stops	SM27	PCc_NEGCON	99%	0.0004
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q22	YES	1.2096	Short	51%		0.000					0.0000
					Open	5%	X	0.060	Prevents contactor closure, stops charge	SM27	PCc_NEGCON	99%	0.0006
					Value change	17%		0.000					0.0000
					Output High	22%	X	0.266	contactor driven, always discharges	SM27	PCc_NEGCON	99%	0.0027
					Output low	5%	X	0.060	Contactor open, prevents charge	SM27	PCc_NEGCON	99%	0.0006
		R35	YES	0.8108	Short	5%		0.000					0.0000
					Open	59%	X	0.478	Contactor open, prevents charge	SM27	PCc_NEGCON	99%	0.0048
					Value change	36%		0.000					0.0000
		C146	YES	0.4029	Short	49%	X	0.197	Collapse 12V, no charge	SM27	PCc_NEGCON	99%	0.0020
					Open	22%	X	0.089	Unstable 12V for HSD	SM27	PCc_NEGCON	99%	0.0009
					Value change	29%		0.000					0.0000
		U35	YES	10	All	50%	X	5.000	prevent contactor control	SM27	PCc_NEGCON	99%	0.0500
					All	50%		0.000					0.0000
		D47	YES	0.4814	Short	49%	X	0.236	Prevent contactor closure, no charge	SM27	PCc_NEGCON	99%	0.0024
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		D48	YES	0.4814	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C149	YES	0.5873	Short	49%	X	0.288	Transient contactor closure	SM27	PCc_NEGCON	99%	0.0029
					Open	22%	X	0.129	EMC performance	SM27	PCc_NEGCON	99%	0.0013
					Value change	29%		0.000					0.0000
	HVNEG_N_DO_V_B	J3-14	NO	0	All	50%	X	0.000	HVNEG_N_DO_V_B permanantly	SM27	PCc_NEGCON	99%	0.0000
			NO		All	50%		0.000					0.0000
	HVNEG_N_EN_DO_UC	TMS570 N2HET1[20] pin 141	YES	1.47	All	50%	X	0.735	HVNEG_N_DO_V_B permanantly	SM27	PCc_NEGCON	99%	0.0074
					All	50%		0.000					0.0000
		Q30	YES	0.0746	Open	73%		0.000					0.0000
					Short	27%	X	0.020	HVNEG_N_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0002
		Q29	YES	0.0746	Open	73%		0.000					0.0000
					Short	27%	X	0.020	HVNEG_N_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0002
		R288	YES	0.8108	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R108	YES	0.7785	Short	5%		0.000					0.0000
					Open	59%	X	0.459	sensitive to noise on input	SM27	PCc_NEGCON	99%	0.0046
					Value change	36%		0.000					0.0000
		R222	YES	0.8377	Short	5%		0.000	HVNEG_N_AI_A_UC measures incorrect current in HVNEG_N_DO_V_B				0.0000
					Open	59%		0.000	HVNEG_N_DO_V_B willnot turn on, HVNEG_N_AI_A_UC measures incorrect current in HVNEG_N_DO_V_B				0.0000
					Value change	36%		0.000	HVNEG_N_AI_A_UC measures incorrect current in HVNEG_N_DO_V_B				0.0000
					Short	51%	X	0.617	HVNEG_N_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0062

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
		Q16	YES	1.2096	Open	5%		0.000					0.0000
					Value change	17%		0.000					0.0000
					Output High	22%		0.000					0.0000
					Output low	5%	X	0.060	HVNEG_N_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0006
		C165	YES	0.5873	Short	49%	X	0.288	HVNEG_N_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0029
					Open	22%		0.000	Reduced EMC Performance				0.0000
					Value change	29%		0.000					0.0000
		D51	NO	0	Short	20%		0.000					0.0000
					Open	45%		0.000					0.0000
					Value change	35%		0.000					0.0000
		TMS570 ADIN[18] pin 62	YES	1.47	All	50%		0.000	HVNEG_N_AI_A_UC measures incorrect current in				0.0000
					All	50%		0.000					0.0000
	HVNEG_N_AI_A_UC	U21	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		C166	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R271	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R272	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C205	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
HV Measurement	HV PSU 9V	C70	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C71	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		L4	X	0	Short	42%		0.000					0.0000
					Open	42%		0.000					0.0000
					Value change	16%		0.000					0.0000
		C72	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C73	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		U12	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		C74	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		L5	X	0	Short	42%		0.000					0.0000
					Open	42%		0.000					0.0000
					Value change	16%		0.000					0.0000
		C75	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C77	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		U11	X	0	All	50%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
		[illegible]			All	50%		0.000					0.0000
		C76	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	Microcontroller and associated decoupling	U13	X	0	All	50%		0.000					0.0000
					All	50%		0.000					
		C86	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C84	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R82	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	Micro reset	RE3/MCLR/VPP	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	IDE header	J9-1	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	IDE header	J9-2	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	IDE header	J9-3	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	IDE header	J9-4	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	IDE header	J9-5	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	Xtal and decouple	X2	X	0	Open	89%		0.000					0.0000
					No oscillation	11%		0.000					0.0000
		C88	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C89	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	HV_TX_DO_UC	CK1/CANTX/RC6 pin17	X	0									0.0000
		Q7	X	0									0.0000
													0.0000
													0.0000
													0.0000
													0.0000
		R90	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		OPTO3	X	0									0.0000
		C90	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C91	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		R258	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	HV_RX_DI_UC	DT1/CANRX/RC7 pin 18	X	0									
		R85	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C87	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		[illegible]	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	29%		0.000					0.0000
		OPTO2	X	0									
		R84	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		Q5	X	0									0.0000
													0.0000
													0.0000
													0.0000
													0.0000
	Analogue Vref	RA3/AN3/Vref+	X	0									
		U14	X	0									
		C83	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		C81	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	HV_SO_9V_AI_V_UC	R83	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R86	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C85	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	HVPOS1_AI_V_B	J8-3	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		R6	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R76	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R77	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R78	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R80	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R81	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C79	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D19	X	0				0.000					0.0000
								0.000					0.0000
								0.000					0.0000
		C78	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	HVPOS1_AI_V_UC	INT0/AN10/RB0	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	HVPOS1_EN_DO_UC	RC1/ISOSCI	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
					Fails to trip	55%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
		RLY1	X	0	Spurious trip	26%		0.000					0.0000
					Short	19%		0.000					0.0000
		Q4	X	0									0.0000
													0.0000
													0.0000
													0.0000
		OPTO1	X	0									
		R79	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
	HVPOS1_AI_V_B	J8-9	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		R50	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R49	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R48	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R47	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R46	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R51	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C61	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D14	X	0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C60	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	HVPOS3_AI_V_UC	RA1/AN1	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	HVPOS4_AI_V_B	J8-8	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		R56	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R55	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R54	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R53	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R52	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R67	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	36%		0.000					0.0000
		C63	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D15	X	0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C62	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	HVPOS4_AI_V_UC	RA5/AN4	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	HVPOS5_AI_V_B	J8-12	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		R62	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R61	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R60	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R59	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R58	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R63	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C65	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D16	X	0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C64	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	HVPOS5_AI_V_UC	INT1/AN8/RB1	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	HVPOS6_AI_V_B	J8-11	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		R68	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R67	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R66	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R65	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R64	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Failure Rate Distribution	Failure mode with potential to violate safety goal	Failure rate based on distribution	Comments	Safety mechanism(s) present to prevent the failure mode from violating the safety goal	Reference	Failure Mode Coverage	Residual or single point fault failure rate / FIT
					Value change	36%		0.000					0.0000
		R69	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C67	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D17	X	0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C66	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	HVPOS6_AI_V_UC	ECCP1/AN9/RB4	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
	HVPOS7_AI_V_B	J8-10	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
		R74	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R73	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R72	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R71	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R70	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		R75	X	0	Short	5%		0.000					0.0000
					Open	59%		0.000					0.0000
					Value change	36%		0.000					0.0000
		C69	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
		D18	X	0	Short	49%		0.000					0.0000
					Open	36%		0.000					0.0000
					Value change	15%		0.000					0.0000
		C68	X	0	Short	49%		0.000					0.0000
					Open	22%		0.000					0.0000
					Value change	29%		0.000					0.0000
	HVPOS7_AI_V_UC	RA0/AN0	X	0	All	50%		0.000					0.0000
					All	50%		0.000					0.0000
Contactors	HVPOS Contactor	HVPOS	Yes	29.383	Fails to trip	55%	X	16.161	Continuous discharge	SM23	PCc_POSCON	99%	0.1616
					Spurious trip	26%	X	7.640	Prevents charge	SM23	PCc_POSCON	99%	0.0764
					Short	19%	X	5.583	Continuous discharge	SM23	PCc_POSCON	99%	0.0558
	HVNEG Contactor	HVNEG	Yes	29.383	Fails to trip	55%	X	16.161	Continuous discharge	SM27	PCc_NEGCON	99%	0.1616
					Spurious trip	26%	X	7.640	Prevents charge	SM27	PCc_NEGCON	99%	0.0764
					Short	19%	X	5.583	Continuous discharge	SM27	PCc_NEGCON	99%	0.0558

Safety Goal: Maintain Voltage Operating Area									LFM Calculation for Architecture 7			
Total FR (FIT)				431.57					Multi point Point (FIT)			40.6406
									Latent Fault Metric			90.30%
System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point Failure Rate (Perceived – Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
Cell / Battery Management	uC, Xtal and supply decoupling	U9	YES	3	All	1.3500	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.1350
					All	1.5000						0.0000
		X1	YES	0.4404	Open	0.3528	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0353
					No oscillation	0.0436	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0044
		C92	YES	0.0585	Short	0.0258	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0026
					Open	0.0116	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0012
					Value change	0.0133	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0015
		C94	YES	0.0585	Short	0.0258	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0026
					Open	0.0116	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0012
					Value change	0.0133	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0015
		R175	YES	0.8564	Short	0.0424	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0042
					Open	0.5002	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0500
					Value change	0.3083						0.0000
		C98	YES	0.489	Short	0.2372						0.0000
					Open	0.1065	X	Other failure prevents correct micro operation or communication	SM1	HWMon	90%	0.0107
					Value change	0.1418						0.0000
		C100	YES	0.2009	Short	0.0974						0.0000
					Open	0.0442	X	ESD loss of protection			0%	0.0442
					Value change	0.0583						0.0000
		C91	YES	0.2009	Short	0.0974						0.0000
					Open	0.0442	X	ESD loss of protection			0%	0.0442
					Value change	0.0583						0.0000
		C84	YES	0.2009	Short	0.0974						0.0000
					Open	0.0442	X	ESD loss of protection			0%	0.0442
					Value change	0.0583						0.0000
		C90	YES	0.2009	Short	0.0974						0.0000
					Open	0.0442	X	ESD loss of protection			0%	0.0442
					Value change	0.0583						0.0000
		C96	YES	0.2009	Short	0.0974						0.0000
					Open	0.0442	X	ESD loss of protection			0%	0.0442
					Value change	0.0583						0.0000
	uC ADC Vdd Supply	L1	YES	0.3828	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C87	YES	0.2009	Short	0.0974						0.0000
					Open	0.0442	X	ESD loss of protection			0%	0.0442
					Value change	0.0583						0.0000
		C107	YES	0.2009	Short	0.0974						0.0000
					Open	0.0442	X	ESD loss of protection			0%	0.0442
					Value change	0.0583						0.0000
	uC ADC Vref	C85	YES	0.2009	Short	0.0974						0.0000
					Open	0.0442	X	ESD loss of protection			0%	0.0442
					Value change	0.0583						0.0000
		C89	YES	0.5696	Short	0.2763						0.0000
					Open	0.1233	X	ESD loss of protection			0%	0.1233
					Value change	0.1632						0.0000
		U17	YES	2.1	All	1.0395	X	3.3V fails high and ADRef is high resulting in same measured voltage within range			0%	1.0395
					All	1.0500						0.0000
	uC Program	J3	NO	0	All	0.0000						0.0000
					All	0.0000						0.0000
	uC Reset	R132	YES	0.7785	Short	0.0385						0.0000
					Open	0.4547						0.0000
					Value change	0.2775						0.0000
		C93	YES	0.1455	Short	0.0706						0.0000
					Open	0.0317						0.0000
					Value change	0.0418						0.0000
					Short	0.0000						0.0000
					Open	0.0000						0.0000

Battery Pack LFM Calculations Sheet 1 of 34

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.0000						0.0000
	External flash memory	R140	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		U7	NO	0		0.0000						0.0000
						0.0000						0.0000
		C81	NO	0	Short	0.0000	X	Other failure stops safety line breaking			0%	0.0000
					Open	0.0000	X	ESD loss of protection			0%	0.0000
					Value change	0.0000						0.0000
		R137	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	uC LED	LED13	NO	0		0.0000						0.0000
						0.0000						0.0000
		R136	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	5V supply potential divider to ADC	R159	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R154	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C99	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	3V3 supply potential divider to ADC	R157	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R158	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C76	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	uC temperature measurement to ADC	R138	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R135	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C77	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	CAN	U15	YES	0.9	All	0.4455	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0045
					All	0.4500						0.0000
		C132	YES	0.0618	Short	0.0300	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0003
			YES		Open	0.0136						0.0000
			YES		Value change	0.0179						0.0000
		C133	YES	0.0618	Short	0.0300	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0003
			YES		Open	0.0136						0.0000
			YES		Value change	0.0179						0.0000
		L5	YES	0.0011	Short	0.0004	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0000
			YES		Open	0.0004	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0000
			YES		Value change	0.0002	X	ESD loss of protection			0%	0.0002
		D66A	YES	2.34	Short	0.4633	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0046
			YES		Open	1.0530	X	ESD loss of protection			0%	1.0530
			YES		Value change	0.8190						0.0000
		D66B	YES	2.34	Short	0.4633	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0046
			YES		Open	1.0530	X	ESD loss of protection			0%	1.0530
			YES		Value change	0.8190						0.0000
		C131	YES	0.0645	Short	0.0128	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0001
			YES		Open	0.0329	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0003
			YES		Value change	0.0187						0.0000
		C129	YES	0.2773	Short	0.0549	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0005
			YES		Open	0.1414	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0014
			YES		Value change	0.0804						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived Latent)	Failure mode that may lead to the violation of safety goal in combination with an independent failure of another component?	Comments	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
			YES		Short	0.0974	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0010
		C130	YES	0.2009	Open	0.0442	X	ESD loss of protection			0%	0.0442
			YES		Value change	0.0583						0.0000
		J1-5	YES	0.0081	All	0.0040	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0000
			YES		All	0.0041						0.0000
		J1-1	YES	0.0081	All	0.0040	X	SM Can failure fails to detect CBM CAN failure	SM2	CAN	99%	0.0000
			YES		All	0.0041						0.0000
		U1	YES	20.81	All	10.3010	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	1.0301
			YES		All	10.4030						0.0000
		R30	YES	0.75	Short	0.0375						0.0000
					Open	0.4380						0.0000
					Value change	0.2700						0.0000
		C9	YES	0.2009	Short	0.0974	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0097
					Open	0.0000	X	ESD loss of protection			0%	0.0000
					Value change	0.0583						0.0000
		D8	YES	13.997	Short	6.8584	X	ESD loss of protection			0%	6.8584
					Open	4.9885	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.4988
					Value change	2.0995						0.0000
		Q4	YES	1.2096	Short	0.6169						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
					Value change	0.2036						0.0000
					Output low	0.2635	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0263
					Output high	0.0605						0.0000
		R35	YES	2.3096	Short	0.1143	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0114
					Open	1.3626						0.0000
					Value change	0.8314						0.0000
		R32	YES	0.9387	Short	0.0469						0.0000
					Open	0.5483	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0548
					Value change	0.3379						0.0000
	6803 Cell Voltage Measurement	Q5	YES	1.2096	Short	0.6169						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
					Value change	0.2036						0.0000
					Output low	0.2661						0.0000
					Output high	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
		C12	YES	0.2009	Short	0.0974	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0097
					Open	0.0442	X	ESD loss of protection			0%	0.0442
					Value change	0.0583						0.0000
		R38	YES	2.3096	Short	0.1143	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0114
					Open	1.3626						0.0000
					Value change	0.8314						0.0000
		R40	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R13	YES	0.8564	Short	0.0424	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0042
					Open	0.5053						0.0000
					Value change	0.3083						0.0000
		C3	YES	0.5696	Short	0.2763	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0276
					Open	0.1253						0.0000
					Value change	0.1652						0.0000
		R11	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
					Short	0.1675	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0167
					Open	0.1253						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.1652						0.0000
	6803 Temp Measurement (on PCB)	R14	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R1	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C2	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	6803 Cell Measurement SPI Comms (pull ups and series resistors)	R16	YES	0.9387	Short	0.0465	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0046
					Open	0.5538						0.0000
					Value change	0.3379						0.0000
		R24	YES	0.9387	Short	0.0465	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0046
					Open	0.5538						0.0000
					Value change	0.3379						0.0000
		R23	YES	0.9387	Short	0.0465	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0046
					Open	0.5538						0.0000
					Value change	0.3379						0.0000
		R17	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R13	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R26	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R25	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R141	YES	0.7785	Short	0.0385						0.0000
					Open	0.4593						0.0000
					Value change	0.2803						0.0000
	6803 Temperature to uC ADC Filter	R3	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C97	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	6803 Vref to uC ADC Filter	R7	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C101	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	Cell 12 clamp voltage	L3	YES	0.3828	Short	0.1608						0.0000
					Open	0.1592	X	Micro fails to act on data discrepancy	SM11		90%	0.0159
					Value change	0.0612						0.0000
		C120	YES	0.6945	Short	0.3369	X	Micro fails to act on data discrepancy	SM11		90%	0.0337
					Open	0.1528						0.0000
					Value change	0.2014						0.0000
		D64	YES	13.997	Short	6.7898	X	Micro fails to act on data discrepancy	SM11		90%	0.6790
					Open	5.0388						0.0000
					Value change	2.0993						0.0000
		D63	YES	13.997	Short	6.7898	X	Micro fails to act on data discrepancy	SM11		90%	0.6790
					Open	5.0388						0.0000
					Value change	2.0993						0.0000
		D62	YES	0.72	Short	0.3493	X	Micro fails to act on data discrepancy	SM11		90%	0.0349
					Open	0.2592						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.1080						0.0000
		R176	NO	0	Short	0.0000	X	Micro fails to act on data discrepancy	SM11		90%	0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R177	YES	0.001	Short	0.0003	X	Micro fails to act on data discrepancy	SM11		90%	0.0000
					Open	0.0000						0.0000
					Value change	0.0002						0.0000
	Cell 12 Filter	R172	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R82	YES	0.727	Short	0.0360						0.0000
					Open	0.0000	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0000
					Value change	0.2617						0.0000
		LED12	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
		R97	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q22	YES	1.2096	Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
					Value change	0.2056						0.0000
					Output low	0.2661						0.0000
					Output high	0.0603						0.0000
		D36	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R98	YES	0.7952	Short	0.0398						0.0000
					Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0464
					Value change	0.2863						0.0000
		C117	YES	1.3233	Short	0.6484						0.0000
					Open	0.2911						0.0000
					Value change	0.3838						0.0000
		D57	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
	Cell 11 Filter	R171	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R100	YES	0.727	Short	0.0360						0.0000
					Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0425
					Value change	0.2617						0.0000
		LED11	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
		R102	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q16	YES	1.2096	Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
					Value change	0.2056						0.0000
					Output low	0.2661						0.0000
					Output high	0.0603						0.0000
		D34	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R86	YES	0.7952	Short	0.0398						0.0000
					Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0464
					Value change	0.2863						0.0000
		C112	YES	1.3233	Short	0.6484						0.0000
					Open	0.2911						0.0000
					Value change	0.3838						0.0000
		[illegible]	[illegible]	[illegible]	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.2520						0.0000
					Short	0.0405						0.0000
		R88	YES	0.8108	Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0474
					Value change	0.2919						0.0000
					Short	0.0363						0.0000
		R105	YES	0.727	Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0425
					Value change	0.2617						0.0000
		LED10	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
		R107	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q15	YES	1.2096	Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
	Cell 10 Filter				Value change	0.2036						0.0000
					Output low	0.2661						0.0000
					Output high	0.0605						0.0000
		D33	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R73	YES	0.7952	Short	0.0398						0.0000
					Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0464
					Value change	0.2863						0.0000
		C104	YES	1.3233	Short	0.6484						0.0000
					Open	0.2911						0.0000
					Value change	0.3838						0.0000
		D55	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R170	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R111	YES	0.727	Short	0.0363						0.0000
					Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0425
					Value change	0.2617						0.0000
		LED9	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
		R114	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q14	YES	1.2096	Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
	Cell 9 Filter				Value change	0.2036						0.0000
					Output low	0.2661						0.0000
					Output high	0.0605						0.0000
		D32	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R72	YES	0.7952	Short	0.0398						0.0000
					Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0464
					Value change	0.2863						0.0000
		C103	YES	1.3233	Short	0.6484						0.0000
					Open	0.2911						0.0000
					Value change	0.3838						0.0000
		D54	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R61	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R128	YES	0.727	Short	0.0363						0.0000
					Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0425

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.2617						0.0000
		LED8	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
		R143	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q8	YES	1.2096	Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0060
					Value change	0.2036						0.0000
	Cell 8 Filter				Output low	0.2661						0.0000
					Output high	0.0605						0.0000
		D22	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R60	YES	0.7952	Short	0.0398						0.0000
					Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0464
					Value change	0.2863						0.0000
		C102	YES	1.3233	Short	0.6484						0.0000
					Open	0.2911						0.0000
					Value change	0.3838						0.0000
		D53	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R129	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R133	YES	0.727	Short	0.0363						0.0000
					Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0425
					Value change	0.2617						0.0000
		LED7	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
		R135	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q35	YES	1.2096	Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0060
					Value change	0.2036						0.0000
	Cell 7 Filter				Output low	0.2661						0.0000
					Output high	0.0605						0.0000
		D52	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R131	YES	0.7952	Short	0.0398						0.0000
					Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0464
					Value change	0.2863						0.0000
		C11	YES	1.3233	Short	0.6484						0.0000
					Open	0.2911						0.0000
					Value change	0.3838						0.0000
		D7	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R48	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R38	YES	0.727	Short	0.0363						0.0000
					Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0425
					Value change	0.2617						0.0000
		LED6	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
		R78	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
					Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0060

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
	Cell 6 Filter	Q34	YES	1.2096	Value change	0.2036						0.0000
					Output low	0.2661						0.0000
					Output high	0.0605						0.0000
		D51	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R148	YES	0.7932	Short	0.0398						0.0000
					Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0464
					Value change	0.2863						0.0000
		C10	YES	1.3233	Short	0.6484						0.0000
					Open	0.2911						0.0000
					Value change	0.3838						0.0000
		D6	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
	Cell 5 Filter	R34	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R83	YES	0.727	Short	0.0363						0.0000
					Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0425
					Value change	0.2617						0.0000
		LED5	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
		R99	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q31	YES	1.2096	Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
					Value change	0.2036						0.0000
					Output low	0.2661						0.0000
					Output high	0.0605						0.0000
		D50	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
		R134	YES	0.7932	Short	0.0398						0.0000
					Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0464
					Value change	0.2863						0.0000
		C8	YES	1.3233	Short	0.6484						0.0000
					Open	0.2911						0.0000
					Value change	0.3838						0.0000
		D5	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000
	Cell 4 Filter	R31	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0474
					Value change	0.2919						0.0000
		R101	YES	0.727	Short	0.0363						0.0000
					Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0425
					Value change	0.2617						0.0000
		LED4	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
		R103	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q30	YES	1.2096	Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
					Value change	0.2036						0.0000
					Output low	0.2661						0.0000
					Output high	0.0605						0.0000
		D49	YES	0.72	Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
					Open	0.3240						0.0000
					Value change	0.2520						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Short	0.0398						0.0000
		R130	YES	0.7952	Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0464
					Value change	0.2863						0.0000
					Short	0.6484						0.0000
		C7	YES	1.3233	Open	0.2911						0.0000
					Value change	0.3838						0.0000
					Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
		D4	YES	0.72	Open	0.3240						0.0000
					Value change	0.2520						0.0000
					Short	0.0405						0.0000
		R10	YES	0.8108	Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0474
					Value change	0.2919						0.0000
					Short	0.0363						0.0000
		R106	YES	0.727	Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0425
					Value change	0.2617						0.0000
		LED3	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
					Short	0.0000						0.0000
		R108	NO	0	Open	0.0000						0.0000
					Value change	0.0000						0.0000
					Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
	Cell 3 Filter	Q28	YES	1.2096	Value change	0.2056						0.0000
					Output low	0.2661						0.0000
					Output high	0.0603						0.0000
					Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
		D43	YES	0.72	Open	0.3240						0.0000
					Value change	0.2520						0.0000
					Short	0.0398						0.0000
		R119	YES	0.7952	Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0464
					Value change	0.2863						0.0000
					Short	0.6484						0.0000
		C3	YES	1.3233	Open	0.2911						0.0000
					Value change	0.3838						0.0000
					Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
		D1	YES	0.72	Open	0.3240						0.0000
					Value change	0.2520						0.0000
					Short	0.0405						0.0000
		R4	YES	0.8108	Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0474
					Value change	0.2919						0.0000
					Short	0.0363						0.0000
		R112	YES	0.727	Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0425
					Value change	0.2617						0.0000
		LED2	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
					Short	0.0000						0.0000
		R115	NO	0	Open	0.0000						0.0000
					Value change	0.0000						0.0000
					Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0060
	Cell 2 Filter	Q27	YES	1.2096	Value change	0.2056						0.0000
					Output low	0.2661						0.0000
					Output high	0.0603						0.0000
					Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
		D39	YES	0.72	Open	0.3240						0.0000
					Value change	0.2520						0.0000
					Short	0.0398						0.0000
		R113	YES	0.7952	Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0464
					Value change	0.2863						0.0000
					Short	0.6484						0.0000
		C1	YES	1.3233	Open	0.2911						0.0000
					Value change	0.3838						0.0000
			YES		Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Sel test PWR L	90%	0.0143
			YES		Open	0.3240						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
			YES		Value change	0.2520						0.0000
					Short	0.0405						0.0000
		R2	YES	0.8108	Open	0.4736	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0474
					Value change	0.2919						0.0000
					Short	0.0363						0.0000
		R131	YES	0.727	Open	0.4246	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0425
					Value change	0.2617						0.0000
		LED1	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
					Short	0.0000						0.0000
		R149	NO	0	Open	0.0000						0.0000
					Value change	0.0000						0.0000
					Short	0.6107						0.0000
					Open	0.0599	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0060
	Cell 1 Filter	Q26	YES	1.2096	Value change	0.2056						0.0000
					Output low	0.2661						0.0000
					Output high	0.0605						0.0000
					Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0143
		D38	YES	0.72	Open	0.3240						0.0000
					Value change	0.2520						0.0000
					Short	0.0398						0.0000
		R109	YES	0.7952	Open	0.4645	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0464
					Value change	0.2863						0.0000
					Short	0.6484						0.0000
		C4	YES	1.3233	Open	0.2911						0.0000
					Value change	0.3838						0.0000
					Short	0.1426	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0143
		D3	YES	0.72	Open	0.3240						0.0000
					Value change	0.2520						0.0000
		J4-1	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-2	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-3	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-4	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-5	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-6	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-7	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-8	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
	Cell connections	J4-9	NO	0	All	0.0000						0.0000
					All	0.0000						0.0000
		J4-10	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-11	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-12	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-13	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-14	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-15	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		J4-16	YES	0.0562	All	0.0278	X	Micro fails to act on data discrepancy	SM11	afety Self test PWR L	90%	0.0028
					All	0.0281						0.0000
		R168	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R169	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		L4	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
					Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		[illegible]	[illegible]		Value change	0.0000						0.0000
	DC-DC Converter Power CBM from Cell stack (Battery Supply)	C126	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C127	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R167	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C123	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R165	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C122	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		U13	NO	0	All	0.0000						0.0000
					All	0.0000						0.0000
		C121	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D65	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C124	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R166	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R164	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		L2	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C118	NO	0	Short	0.0000	X	Other failure stops safety line breaking			0%	0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C119	NO	0	Short	0.0000	X	Other failure stops safety line breaking			0%	0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	5V Power Supply	C136	YES	0.0643	Short	0.0313	X	Other failure stops safety line breaking			0%	0.0313
					Open	0.0142						0.0000
					Value change	0.0187						0.0000
		C79	YES	0.2009	Short	0.1134	X	Other failure stops safety line breaking			0%	0.1134
					Open	0.0643						0.0000
					Value change	0.0221						0.0000
		U16	YES	10	All	4.9300	X	Other failure stops safety line breaking			0%	4.9300
					All	5.0000						0.0000
		C135	YES	0.0643	Short	0.0364	X	Other failure stops safety line breaking			0%	0.0364
					Open	0.0206						0.0000
					Value change	0.0071						0.0000
		C88	YES	0.2009	Short	0.1134	X	Other failure stops safety line breaking			0%	0.1134
					Open	0.0643						0.0000
					Value change	0.0221						0.0000
		L6	YES	0.0011	Short	0.0003						0.0000
					Open	0.0004	X	Other failure stops safety line breaking			0%	0.0004
					Value change	0.0002						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
	5V Isolated Supply	C39	YES	0.2009	Short	0.0974	X	Other failure stops safety line breaking			0%	0.0974
					Open	0.0442						0.0000
					Value change	0.0583						0.0000
		U3	YES	3	All	1.4850	X	Other failure stops safety line breaking			0%	1.4850
					All	1.5000						0.0000
		C60	YES	0.387	Short	0.1878	X	Other failure stops safety line breaking			0%	0.1878
					Open	0.0852						0.0000
					Value change	0.1122						0.0000
		C58	YES	0.387	Short	0.1878	X	Other failure stops safety line breaking			0%	0.1878
					Open	0.0852						0.0000
					Value change	0.1122						0.0000
		D35	YES	13.997	Short	6.8584						0.0000
					Open	4.9885	X	Other failure stops safety line breaking			0%	4.9885
					Value change	2.0993						0.0000
	3V3 Power Supply	C110	YES	0.2773	Short	0.1345	X	Other failure stops safety line breaking			0%	0.1345
					Open	0.0610						0.0000
					Value change	0.0804						0.0000
		U11	YES	0.4432	All	0.2194	X	Other failure stops safety line breaking			0%	0.2194
					All	0.2216						0.0000
		C105	YES	0.2009	Short	0.0974	X	Other failure stops safety line breaking			0%	0.0974
					Open	0.0442						0.0000
					Value change	0.0583						0.0000
		C109	YES	10.936	Short	6.1711	X	Other failure stops safety line breaking			0%	6.1711
					Open	3.4995						0.0000
					Value change	1.2029						0.0000
	Safety Monitor Cell 12	R174	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C52	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D28	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor Cell 11	R173	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C49	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D27	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor Cell 10	R87	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C50	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D26	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor Cell 9	R77	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C47	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D24	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
		R63	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
	Safety Monitor Cell 8	C41	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D23	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor Cell 7	R121	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C69	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D47	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor Cell 6	R147	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C68	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D42	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor Cell 5	R133	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C64	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D46	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor Cell 4	R127	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C71	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D41	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor Cell 3	R117	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C67	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D45	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor Cell 2	R116	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C66	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253
		D40	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor Cell 1	R118	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C65	YES	0.1455	Short	0.0428						0.0000
					Open	0.0192	X	Other failure stops safety line breaking			0%	0.0192
					Value change	0.0253	X	Other failure stops safety line breaking			0%	0.0253

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		D44	YES	0.72	Short	0.0864						0.0000
					Open	0.1944	X	Other failure stops safety line breaking			0%	0.1944
					Value change	0.2520						0.0000
	Safety Monitor	U5	YES	20.81	All	10.4050	X	In conjunction with 6803 micro	SM12	Wdog	90%	1.0405
					All	5.2025						0.0000
		R122	YES	0.8108	Short	0.0243	X	Other failure stops safety line breaking			0%	0.0243
					Open	0.2870						0.0000
					Value change	0.2919						0.0000
		C73	YES	1.3233	Short	0.3891						0.0000
					Open	0.1747	X	Other failure stops safety line breaking			0%	0.1747
					Value change	0.2303	X	Other failure stops safety line breaking			0%	0.2303
		C74	YES	0.5696	Short	0.1675						0.0000
					Open	0.0752	X	Other failure stops safety line breaking			0%	0.0752
					Value change	0.1632						0.0000
		C72	YES	0.5696	Short	0.1675						0.0000
					Open	0.0752	X	Other failure stops safety line breaking			0%	0.0752
					Value change	0.1632						0.0000
		R125	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R9	YES	2.3096	Short	0.1155						0.0000
					Open	0.0000	X	Other failure stops safety line breaking			0%	0.0000
					Value change	0.8314						0.0000
	Internal LTC temperature	C70	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C62	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R120	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R110	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	External LTC temperature	C78	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R160	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		J4-9	NO	0	All	0.0000						0.0000
					All	0.0000						0.0000
	Safety Line	D48	YES	1.2	Short	0.5821						0.0000
					Open	0.4277						0.0000
					Value change	0.1782						0.0000
		C75	YES	0.2009	Short	0.0974						0.0000
					Open	0.0437						0.0000
					Value change	0.0577						0.0000
		R123	YES	2.3096	Short	0.1143						0.0000
					Open	1.3490						0.0000
					Value change	0.8231						0.0000
		Q29	YES	1.2096	Short	0.6107						0.0000
					Open	0.0599						0.0000
					Value change	0.2036						0.0000
					Output low	0.2633						0.0000
					Output high	0.0599						0.0000
		R126	YES	2.3096	Short	0.1143						0.0000
					Open	1.3490						0.0000
					Value change	0.8231						0.0000
		C139	YES	0.0744	Short	0.0361						0.0000
					Open	0.0164						0.0000
					Value change	0.0214						0.0000
					Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Revised + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		R224			Value change	0.0000						0.0000
		C140	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	Safety Relay	RLY1	YES	0.6612	Fails to trip	0.3600						0.0000
					Spurious trip	0.0000						0.0000
					Short	0.0000						0.0000
		R89	YES	0.7263	Short	0.0359						0.0000
					Open	0.4242						0.0000
					Value change	0.2613						0.0000
String Management Low Voltage	Power Supply	J3-1 PERM_SI_12V_B	NO	0	All	0.0000						0.0000
					All	0.0000						0.0000
		J1-20 0V	NO	0	All	0.0000						0.0000
					All	0.0000						0.0000
		U39	YES	10	All	4.5000						0.0000
					All	0.0000						0.0000
		C209	YES	0.5873	Short	0.2878						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D56	YES	4.4928	Short	0.8986						0.0000
					Open	1.8196						
					Value change	1.5723						
		R227		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R229		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D58		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q18		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
		R228		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D29		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D57		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q17		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
					Output low	0.0000						0.0000
					Output high	0.0000						0.0000
		R231		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C212		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C208	YES	0.2009	Short	0.0984						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
					Short	0.0082						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		L9	YES	0.0216	open	0.0091						0.0000
					Value change	0.0035						0.0000
		C210	YES	0.2009	Short	0.0984						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C211	YES	0.0645	Short	0.0316						0.0000
					Open	0.0128						0.0000
					Value change	0.0187						0.0000
		C174	YES	0.0645	Short	0.0316						0.0000
					Open	0.0128						0.0000
					Value change	0.0187						0.0000
		C175	YES	0.0645	Short	0.0316						0.0000
					Open	0.0128						0.0000
					Value change	0.0187						0.0000
		R103	YES	2.3096	Short	0.1155						0.0000
					Open	1.3490						0.0000
					Value change	0.8314						0.0000
		U40	NO	0	All	0.0000						0.0000
					All	0.0000						0.0000
		R230	YES	0.7785	Short	0.0350						0.0000
					Open	0.4593						0.0000
					Value change	0.2803						0.0000
		R232	YES	0.7785	Short	0.0350						0.0000
					Open	0.4593						0.0000
					Value change	0.2803						0.0000
		R233	YES	0.7785	Short	0.0350						0.0000
					Open	0.4593						0.0000
					Value change	0.2803						0.0000
		R14	YES	0.8108	Short	0.0365						0.0000
					Open	0.4784						0.0000
					Value change	0.2919						0.0000
		C213		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R234	YES	0.7195	Short	0.0360						0.0000
					Open	0.4203						0.0000
					Value change	0.2590						0.0000
		R235	No	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C215	No	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R328	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.0000						0.0000
		R240	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R104	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R106	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C219	Yes	0.5873	Short	0.2590						0.0000
					Open	0.1163						0.0000
					Value change	0.1703						0.0000
		L10	YES	0.0017	Short	0.0007						0.0000
					Open	0.0007						0.0000
					Value change	0.0002						0.0000
		D59	YES	1.6542	Short	0.7293						0.0000
					Open	0.5360						0.0000
					Value change	0.2233						0.0000
		C16		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R284		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C214		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q19		0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
					Output High	0.0000						
					Output low	0.0000						
		R236		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R237		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R239		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C216		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C217	Yes	0.7269	Short	0.3206						0.0000
					Open	0.1439						0.0000
					Value change	0.2108						0.0000
		C218	Yes	1.6809	Short	0.7413						0.0000
					Open	0.3328						0.0000
					Value change	0.4873						0.0000
		C206	Yes	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C220	No	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		C97	No	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	Microcontroller and associated decoupling	U8	Yes	1.47	All	0.7277						0.0000
					All	0.7350						0.0000
		C53	Yes	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C54	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C55	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C56	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C50	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C47	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C46	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C44	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C42	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C40	YES	0.5696	Short	0.2512						0.0000
					Open	0.1128						0.0000
					Value change	0.1652						0.0000
		L3	YES	0.3828	Short	0.1447						0.0000
					Open	0.1447						
					Value change	0.0612						
		C248	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C36	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C35	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C34	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C41	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C43	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C45	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C48	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
					Short	0.0886						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		C49	YES	0.2009	Open	0.0398						0.0000
					Value change	0.0583						0.0000
		C51	YES	0.2009	Short	0.0886						0.0000
					Open	0.0398						0.0000
					Value change	0.0583						0.0000
	Micro Oscillator	X1	NO	0	Open	0.0000						0.0000
					No Oscillation	0.0000						0.0000
		R44	YES	0.8564	Short	0.0428						0.0000
					Open	0.5033						0.0000
					Value change	0.3052						0.0000
		R45	YES	0.7722	Short	0.0386						0.0000
					Open	0.4556						0.0000
					Value change	0.2752						0.0000
		C57	YES	0.0585	Short	0.0287						0.0000
					Open	0.0129						0.0000
					Value change	0.0168						0.0000
		C59	YES	0.0585	Short	0.0287						0.0000
					Open	0.0129						0.0000
					Value change	0.0168						0.0000
	Micro ADC reference	U7	NO	0	Open	0.0000						0.0000
					Short	0.0000						0.0000
					Value Change	0.0000						
		D61	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C37	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C39	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	Jtag	J7-1	YES	0.05	All	0.0248						0.0000
					All	0.0250						0.0000
		J7-2	YES	0.05	All	0.0248						0.0000
					All	0.0250						0.0000
		J7-3	YES	0.05	All	0.0248						0.0000
					All	0.0250						0.0000
		J7-4	YES	0.05	All	0.0248						0.0000
					All	0.0250						0.0000
		J7-5	YES	0.05	All	0.0248						0.0000
					All	0.0250						0.0000
		J7-6	YES	0.05	All	0.0248						0.0000
					All	0.0250						0.0000
	Battery CAN	C222	YES	0.0618	Short	0.0300						0.0000
					Open	0.0136						
					Value change	0.0179						
		R241	YES	0.7629	Short	0.0378						0.0000
					Open	0.4456						0.0000
					Value change	0.2719						0.0000
		R242	YES	0.7629	Short	0.0378						0.0000
					Open	0.4456						0.0000
					Value change	0.2719						0.0000
		D60	YES	2.34	Short	0.4633						0.0000
					Open	1.0530						
					Value change	0.8190						
		C223	YES	0.0618	Short	0.0300						0.0000
					Open	0.0136						0.0000
					Value change	0.0179						0.0000
		[illegible]	[illegible]	[illegible]	Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		C114			Value change	0.0000						0.0000
		L11	YES	0.0331	Short	0.0138						0.0000
					Open	0.0000						
					Value change	0.0053						
		U41	YES	1	All	0.4950						0.0000
					All	0.5000						
		C221	YES	0.489	Short	0.2372						0.0000
					Open	0.1076						0.0000
					Value change	0.1418						0.0000
		J1-22	YES	0.05	All	0.0248						0.0000
					All	0.0250						0.0000
		J1-23	YES	0.05	All	0.0248						0.0000
					All	0.0250						0.0000
		J1-25	YES	0.05	All	0.0248						0.0000
					All	0.0250						0.0000
		J1-26	YES	0.05	All	0.0248						0.0000
					All	0.0250						0.0000
		J6-1	YES	0.0081	All	0.0040						0.0000
					All	0.0041						0.0000
		J6-5	YES	0.0081	All	0.0040						0.0000
					All	0.0041						0.0000
	Vehicle CAN	C11	no	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R3	no	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R4	no	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D3	no	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		C12	no	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C13	no	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		L2	no	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		U2	no	0	All	0.0000						0.0000
					All	0.0000						
		C9	no	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R5	no	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		Q1	no	0	Short	0.0000						0.0000
					Open	0.0000						
		C5	no	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C6	no	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		J1-11	no	0	All	0.0000						0.0000
					All	0.0000						0.0000
		J1-12	no	0	All	0.0000						0.0000
					All	0.0000						0.0000
		SCIRX Pin 38	no	0	All							
	LV_RX_DI_UC	SCITX Pin 39	no		All							
	LV_TX_DO_UC	J1-29		0	All	0.0000						0.0000
					All	0.0000						0.0000
	DISCHG_REQ_DI_V_B	C93		0	Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.0000						0.0000
		R93		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R94		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R92		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R95		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D20		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C92		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		J1-30		0	All	0.0000						0.0000
					All	0.0000						0.0000
	CHG_REQ_DI_V_B	C95		0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		R97		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R98		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R96		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R99		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D21		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C94		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q11		0	Short	0.0000						0.0000
					Open							
	SW-SO_12V_I1, 12V enable from Micro	R201		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R199		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D39		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q10		0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
					Output High	0.0000						
					Output low	0.0000						
		R202		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	SW_SO_12V_AI_V_UC, 12V sense to micro	R204		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		[illegible]		0	Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		[illegible]		[illegible]	Value change	0.0000						0.0000
		D40		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C186		0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		J6-2		0	All	0.0000						0.0000
					All	0.0000						0.0000
	CMB_SO_SVO_B	J6-7	Yes	0.0081	All	0.0040						0.0000
					All	0.0041						0.0000
		C256	Yes	0.2929	Short	0.1435						0.0000
					Open	0.0638						0.0000
					Value change	0.0849						0.0000
		L8	Yes	0.0004	Short	0.0001						0.0000
					Open	0.0002						
					Value change	0.0001						
		C193	Yes	0.3177	Short	0.1557						0.0000
					Open	0.0692						0.0000
					Value change	0.0921						0.0000
		C194	Yes	0.3177	Short	0.1557						0.0000
					Open	0.0692						0.0000
					Value change	0.0921						0.0000
		C195	Yes	0.3177	Short	0.1557						0.0000
					Open	0.0692						0.0000
					Value change	0.0921						0.0000
		C196	Yes	0.3177	Short	0.1557						0.0000
					Open	0.0692						0.0000
					Value change	0.0921						0.0000
		U32	Yes	0.6	All	0.2970						0.0000
					All	0.3000						0.0000
		R208	Yes	0.7895	Short	0.0395						0.0000
					Open	0.4638						0.0000
					Value change	0.2814						0.0000
		R209	Yes	0.7177	Short	0.0359						0.0000
					Open	0.4235						0.0000
					Value change	0.2558						0.0000
		C254	Yes	0.1454	Short	0.0712						0.0000
					Open	0.0320						0.0000
					Value change	0.0417						0.0000
		C197	Yes	0.1467	Short	0.0719						0.0000
					Open	0.0323						0.0000
					Value change	0.0421						0.0000
		D38	Yes	0.197	Short	0.0394						0.0000
					Open	0.0886						0.0000
					Value change	0.0689						0.0000
		L7	Yes	0.0011	Short	0.0004						0.0000
					Open	0.0005						
					Value change	0.0000						
		C190	Yes	0.8617	Short	0.4222						0.0000
					Open	0.1877						0.0000
					Value change	0.2499						0.0000
		C191	Yes	0.8617	Short	0.4222						0.0000
					Open	0.1877						0.0000
					Value change	0.2499						0.0000
		C192	Yes	0.8617	Short	0.4222						0.0000
					Open	0.1877						0.0000
					Value change	0.2499						0.0000
		R13	Yes	0.8556	Short	0.0428						0.0000
					Open	0.5048						0.0000
					Value change	0.3049						0.0000
		R210	Yes	0.7319	Short	0.0366						0.0000
					Open	0.4318						0.0000
					Value change	0.2608						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
	CBM_SO_BV0_EN_DO_UC, enable from micro	Q27	Yes	0.0746	Short	0.0539						0.0000
					Open	0.0201						
		R273	No	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D25	No	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R274	No	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q28	Yes	1.2096	Short	0.6107						
					Open	0.0603						
					Value change	0.2036						
					Output High	0.2661						
					Output low	0.0603						
		C198	No	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		R207	No	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R285	No	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	CBM_SO_BV0_AI_V_UC, BV0 feedback to micro	R100	Yes	0.7785	Short	0.0385						0.0000
					Open	0.4547						0.0000
					Value change	0.2775						0.0000
		R101	Yes	0.7785	Short	0.0385						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C96	Yes	0.2009	Short	0.0974						0.0000
					Open	0.0442						0.0000
					Value change	0.0583						0.0000
	SAFETY_OUT_AO_V_V	R171	Yes	0.7355	Short	0.0364						0.0000
					Open	0.4296						0.0000
					Value change	0.2621						0.0000
	SAFETY_IN_AI_V_B	R176	Yes	0.7355	Short	0.0364						0.0000
					Open	0.4296						0.0000
					Value change	0.2621						0.0000
		R283	Yes	0.7785	Short	0.0385						0.0000
					Open	0.4547						0.0000
					Value change	0.2775						0.0000
		C246	Yes	0.2009	Short	0.0974						0.0000
					Open	0.0437						0.0000
					Value change	0.0583						0.0000
		C247	Yes	0.0764	Short	0.0370						0.0000
					Open	0.0166						0.0000
					Value change	0.0221						0.0000
		D26	Yes	1.4811	Short	0.7185						0.0000
					Open	0.5279						0.0000
					Value change	0.2222						0.0000
		R173	Yes	0.8108	Short	0.0401						0.0000
					Open	0.4736						0.0000
					Value change	0.2890						0.0000
					Short	0.0362						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		R178	Yes	0.7314	Open	0.4272						0.0000
					Value change	0.2607						0.0000
		R181	Yes	0.7319	Short	0.0362						0.0000
					Open	0.4279						0.0000
					Value change	0.2608						0.0000
		U25	Yes	1	All	0.4850						0.0000
					All	0.5000						
		R174	Yes	0.8919	Short	0.0442						0.0000
					Open	0.5262						0.0000
					Value change	0.3211						0.0000
		R175	Yes	0.8919	Short	0.0442						0.0000
					Open	0.5262						0.0000
					Value change	0.3211						0.0000
		R180	Yes	0.8108	Short	0.0405						0.0000
					Open	0.4736						0.0000
					Value change	0.2919						0.0000
		C157		0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		R177		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	SAFETY_OK_DLY_DI_V_UC	C156		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R179		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	SAFETY_OK_DI_V_UC	D33		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R172		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C155		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R169		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	SAFETY_IN_AI_V_UC	R170		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C151		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D32		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C152		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q2		0	Short	0.0000						0.0000
					Open	0.0000						
	HVIL_EN_DO_UC	R10		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		U3		0	All	0.0000						0.0000
					All	0.0000						
		R18		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVIL_OUT_SW_AO_V_B	D7		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		R23		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C24		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C22		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVIL_OUT_AI_A_UC	U4		0	All	0.0000						0.0000
					All							
		C17		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R17		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C20		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R11		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVIL_OUT_SW_AO_V_B	R12		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C14		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D4		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C15		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		J1-1		0	All	0.0000						0.0000
					All	0.0000						0.0000
	HVIL_OUT_SW_AO_	J1-17		0	All	0.0000						0.0000
					All	0.0000						0.0000
	HVIL_OUT_RES_AO_	J1-2		0	All	0.0000						0.0000
					All	0.0000						0.0000
	HVIL_IN_AI_V_B	R26		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R31		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVIL_IN_AI_A_C	R30		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C28		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D9		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C29		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R27		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C27		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R20		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
	HVIL_OK_DI_V_UC	R25		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R32		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		U5		0	All	0.0000						0.0000
					All	0.0000						
		R21		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C23		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R24		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D8		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R19		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C25		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R22		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVIL_OK_DLY_DI_V_UC	R29		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C30		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R28		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C31		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R15		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVIL_IN_SW_AO_V_B	R16		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C18		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D5		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C19		0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		TMS570 N2HET1[16]		0	All							
					All							
	HVPOS1_EN_DO_UC	R289	YES	0.7195	Short	0.0360						0.0000
					Open	0.4245	X	R219 O/C may allow noise to trigger HVPOS1_P_DO_V_B	SM18	elded Contact Chec	99%	0.0042
					Value change	0.2590						0.0000
		U22	X	0	All	0.0000						0.0000
					All	0.0000						
		R219	YES	0.8557	Short	0.0428						0.0000
					Open	0.5049	X	R289 O/C may allow noise to trigger HVPOS1_P_DO_V_B	SM18	elded Contact Chec	99%	0.0050

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.3081						0.0000
		Q14	YES	1.2096	Short	0.6107	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0061
					Open	0.0603						
					Value change	0.2036						
					Output High	0.2661						
					Output low	0.0599	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	
		R217	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D43	NO	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		D44	NO	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		C147	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D41	NO	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		R215	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q12	YES	1.2096	Short	0.6107	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0061
					Open	0.0603						
					Value change	0.2036						
					Output High	0.2635	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	
					Output low	0.0603						
		J3-4	NO	0	All							
					All							
	HVPOS1_AI_A_UC	TMS570 ADIN[19] pin 63	NO	0	All	0.0000						0.0000
					All							
	HVPOS1_P_AI_A_UC	R211	NO	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		U33	NO	0	All	0.0000						0.0000
					All							
		C104	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C98	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R213	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C199	NO	0	Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.0000						0.0000
	HVPOS1_N_DO_V_B	J3-12	YES	0.05	All	0.0248	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0002
					All	0.0000						0.0000
		R36	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0047
					Value change	0.2919						0.0000
		U36	YES	10	All	4.9500	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0495
					All	5.0000						
		D49	YES	0.7879	Short	0.1560	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	
					Open	0.3546						
					Value change	0.2758						
		C130	YES	0.5873	Short	0.2849	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0028
					Open	0.1279	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0013
					Value change	0.1703						0.0000
		J3-6	YES	0.05	All	0.0250						0.0000
					All	0.0250						0.0000
	HVNEG_P_DO_V_B	R221	YES	0.8919	Short	0.0442	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0004
					Open	0.5262						0.0000
					Value change	0.3211						0.0000
		Q22	YES	1.2096	Short	0.6169						0.0000
					Open	0.0599	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	
					Value change	0.2036						
					Output High	0.2635	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	
					Output low	0.0599	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	
		R35	YES	0.8108	Short	0.0405						0.0000
					Open	0.4736	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0047
					Value change	0.2919						0.0000
		C146	YES	0.4029	Short	0.1934	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0020
					Open	0.0878	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0009
					Value change	0.1168						0.0000
		U35	YES	10	All	4.9500	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0495
					All	5.0000						
		D47	YES	0.4814	Short	0.2333	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0023
					Open	0.1733						
					Value change	0.0722						
		D48	YES	0.4814	Short	0.2339						0.0000
					Open	0.1733						
					Value change	0.0722						
		C149	YES	0.5873	Short	0.2849	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0028
					Open	0.1279	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0013
					Value change	0.1703						0.0000
	HVNEG_N_DO_V_B	J3-14	NO	0	All	0.0000	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0000
			NO		All	0.0000						0.0000
	HVNEG_N_EN_DO_UC	TMS570 N2HET1[20] pin 141	YES	1.47	All	0.7277	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0073
					All	0.0000						0.0000
		Q30	YES	0.0746	Open	0.0545						0.0000
					Short	0.0199	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0002
		Q29	YES	0.0746	Open	0.0545						0.0000
					Short	0.0199	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0002
		R288	YES	0.8108	Short	0.0405						0.0000
					Open	0.4784						0.0000
					Value change	0.2919						0.0000
		R108	YES	0.7785	Short	0.0389						0.0000
					Open	0.4547	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0045
					Value change	0.2803						0.0000
		R222	YES	0.8377	Short	0.0419						0.0000
					Open	0.4942						0.0000
					Value change	0.3016						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
		Q16	YES	1.2096	Short	0.6107	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0061
					Open	0.0605						0.0000
					Value change	0.2056						0.0000
					Output High	0.2661						0.0000
					Output low	0.0599	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0006
		C165	YES	0.5873	Short	0.2849	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0028
					Open	0.1292						0.0000
					Value change	0.1703						0.0000
		D51	NO	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		TMS570 ADIN[18] pin 62	YES	1.47	All	0.7350						0.0000
					All	0.7350						
	HVNEG_N_AI_A_UC	U21	X	0	All	0.0000						0.0000
					All	0.0000						
		C166	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R271	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R272	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C205	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
HV Measurement	HV PSU 9V	C70	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C71	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		L4	X	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		C72	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C73	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		U12	X	0	All	0.0000						0.0000
					All	0.0000						
		C74	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		L5	X	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		C75	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C77	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		U11	X	0	All	0.0000						0.0000
					All	0.0000						
		C76	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	Microcontroller and associated	U13	X	0	All	0.0000						0.0000
					All							
		C86	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
	decouplings				Value change	0.0000						0.0000
		C84	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R82	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	Micro reset	RE3/MCLR/VPP	X	0	All	0.0000						0.0000
					All	0.0000						
	IDE header	J9-1	X	0	All	0.0000						0.0000
					All	0.0000						0.0000
	IDE header	J9-2	X	0	All	0.0000						0.0000
					All	0.0000						0.0000
	IDE header	J9-3	X	0	All	0.0000						0.0000
					All	0.0000						0.0000
	IDE header	J9-4	X	0	All	0.0000						0.0000
					All	0.0000						0.0000
	IDE header	J9-5	X	0	All	0.0000						0.0000
					All	0.0000						0.0000
	Xtal and decouple	X2	X	0	Open	0.0000						0.0000
					No oscillation	0.0000						0.0000
		C88	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C89	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HV_TX_DO_UC	CK1/CANTX/RC6 pin17	X	0		0.0000						0.0000
		Q7	X	0		0.0000						0.0000
						0.0000						
						0.0000						
						0.0000						
		R90	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		OPTO3	X	0		0.0000						0.0000
		C90	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C91	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R258	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HV_RX_DI_UC	DT1/CANRX/RC7 pin 18	X	0								
		R85	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C87	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C82	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		OPTO2	X	0								
		R84	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		Q5	X	0		0.0000						
						0.0000						
						0.0000						
						0.0000						
	Analogue Vref	RA3/AN3/Vref+	X	0								
		U14	X	0								
		C83	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C84	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.0000						0.0000
	HV_SO_9V_AI_V_UC	R83	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R86	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C85	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVPOS1_AI_V_B	J8-3	X	0	All	0.0000						0.0000
					All	0.0000						0.0000
		R6	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R76	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R77	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R78	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R80	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R81	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C79	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D19	X	0		0.0000						0.0000
						0.0000						
						0.0000						
		C78	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVPOS1_AI_V_UC	INT0/AN10/RB0	X	0	All	0.0000						
					All	0.0000						
	HVPOS1_EN_DO_UC	RC1/ISOSCI	X	0	All	0.0000						
					All	0.0000						
		RLY1	X	0	Fails to trip	0.0000						0.0000
					Spurious trip	0.0000						0.0000
					Short	0.0000						0.0000
		Q4	X	0		0.0000						
						0.0000						
						0.0000						
						0.0000						
		OPTO1	X	0								
		R79	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVPOS1_AI_V_B	J8-9	X	0	All	0.0000						0.0000
					All	0.0000						
		R50	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R49	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R48	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R47	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R46	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.0000						0.0000
		R51	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C61	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D14	X	0	Short	0.0000						0.0000
					Open	0.0000						
					Value change	0.0000						
		C60	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVPOS3_AI_V_UC	RA1/AN1	X	0	All	0.0000						
					All	0.0000						
	HVPOS4_AI_V_B	J8-8	X	0	All	0.0000						0.0000
					All	0.0000						
		R56	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R55	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R54	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R53	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R52	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R57	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C63	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D15	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C62	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVPOS4_AI_V_UC	RA5/AN4	X	0	All	0.0000						
					All	0.0000						
	HVPOS5_AI_V_B	J8-12	X	0	All	0.0000						0.0000
					All	0.0000						
		R62	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R61	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R60	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R59	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R58	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R63	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C64	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.0000						0.0000
		D16	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C64	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVPOS5_AI_V_UC	INT1/AN8/RB1	X	0	All	0.0000						
					All	0.0000						
	HVPOS6_AI_V_B	J8-11	X	0	All	0.0000						0.0000
					All	0.0000						
		R68	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R67	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R66	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R65	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R64	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R69	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C67	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D17	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C66	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
	HVPOS6_AI_V_UC	ECCP1/AN9/RB4	X	0	All	0.0000						
					All	0.0000						
	HVPOS7_AI_V_B	J8-10	X	0	All	0.0000						0.0000
					All	0.0000						
		R74	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R73	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R72	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R71	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R70	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		R75	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		C69	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		D18	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000
					Value change	0.0000						0.0000
		[illegible]	X	0	Short	0.0000						0.0000
					Open	0.0000						0.0000

System	Sub-System	Component Name	Safety Related Component?	Safety Related (SR) Failure Rate / FIT	Failure Mode	Multi point failure Rate (Perceived + Latent)	Failure mode that may lead to the violation of safety goal in combination with an independant failure of another component?	Comments	Detection means ? Safety mechanism(s) present to prevent the failure mode from being latent	Reference	Failure Mode Coverage	Latent multiple point failure rate / FIT
					Value change	0.0000						0.0000
	HVPOS7_AI_V_UC	RAD/ANO	X	0	All	0.0000						0.0000
					All	0.0000						0.0000
Contactors	HVPOS Contactor	HVPOS	Yes	29.383	Fails to trip	15.9992	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.1600
					Spurious trip	7.5632	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0756
					Short	5.5270	X	HVNEG_P_DO_V_B permanantly enabled	SM27	PCc_NEGCON	99%	0.0553
	HVNEG Contactor	HVNEG	Yes	29.383	Fails to trip	15.9992	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.1600
					Spurious trip	7.5632	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0756
					Short	5.5270	X	HVPOS_P_DO_V_B permanantly enabled	SM23	PCc_POSCON	99%	0.0553

Appendix F – FCCS – Candidate Architecture DC% Claims

Table 171: FCCS - Actuator 1

Reference	1)A1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCc
		100%			71.70%	Low	71.55%	Low	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
										Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																		
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	40%	24%	24%	Y		➤	Y											PCc_HVNEG
		Welded Contacts	Welded Contacts	Welded Contacts	30%	18%	18%	Y		➤	Y											PCc_HVNEG
			Individual welded contacts	Individual welded contacts	0%	0%	0%			➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y				➤		➤	y							PCc_PSU_Mon
			Drift	Drift & Oscillation	15%	15%	15%	Y				➤		➤	y							PCc_PSU_Mon
				Power Spikes	5%	5%	5%	Y				➤		➤	y							PCc_PSU_Mon
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	0%	0%	0%							➤				➤		➤		
				Incorrect action	0%	0%	0%							➤				➤		➤		
				Delayed Action	0%	0%	0%							➤				➤		➤		
										42.00%		0.00%		29.70%		0%		0%		0%		

Table 172: FCCS - Actuator 2

Reference	1)A2	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%			71.70%	Low	71.55%	Low	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
										Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																		
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	40%	24%	24%	Y		➤	Y											PCc_HVPOS
		Welded Contacts	Welded Contacts	Welded Contacts	30%	18%	18%	Y		➤	Y											PCc_HVPOS
			Individual welded contacts	Individual welded contacts	0%	0%	0%			➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y				➤		➤	y							PCc_PSU_Mon
			Drift	Drift & Oscillation	15%	15%	15%	Y				➤		➤	y							PCc_PSU_Mon
				Power Spikes	5%	5%	5%	Y				➤		➤	y							PCc_PSU_Mon
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	0%	0%	0%									➤	Y	➤		➤		
				Incorrect action	0%	0%	0%									➤	Y	➤		➤		
				Delayed Action	0%	0%	0%									➤	Y	➤		➤		
										42.00%		0.00%		29.70%		0%		0%		0%		

Table 173: FCCS - Actuator 3

Reference	1)A3	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%			60.00%	Low	59.40%	Limited	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
										Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																		
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	0%	0%	0%			➤												
		Welded Contacts	Welded Contacts	Welded Contacts	0%	0%	0%			➤												
			Individual welded contacts	Individual welded contacts	0%	0%	0%			➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	0%	0%	0%					➤		➤								
			Drift	Drift & Oscillation	0%	0%	0%					➤		➤								
				Power Spikes	0%	0%	0%					➤		➤								
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	100%	60%	59%	y								➤	Y	➤		➤		PCc_FAN's'_SPEED
				Incorrect action	0%	0%	0%									➤		➤		➤		
				Delayed Action	0%	0%	0%									➤		➤		➤		
										0.00%		0.00%		0.00%		60%		0%		0%		

Table 174: FCCS - Actuator 4

Reference	1)A4	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			99.00%	High	99.00%	High	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
										Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																		
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	0%	0%	0%			➤												
		Welded Contacts	Welded Contacts	Welded Contacts	0%	0%	0%			➤												
			Individual welded contacts	Individual welded contacts	0%	0%	0%			➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	0%	0%	0%					➤		➤								
			Drift	Drift & Oscillation	0%	0%	0%					➤		➤								
				Power Spikes	0%	0%	0%					➤		➤								
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	30%	30%	30%	Y								➤	Y	➤		➤	Y	PCc_FAN's'_SPEED
				Incorrect action	40%	40%	40%	Y								➤	Y	➤		➤	Y	PCc_FAN's'_SPEED
				Delayed Action	30%	30%	30%	Y								➤	Y	➤		➤	Y	PCc_FAN's'_SPEED
										0.00%		0.00%		0.00%		60%		0%		99%		

Table 175: FCCS - Actuator 7

Reference	1)A7	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			99.00%	High	99.00%	High	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
										Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																		
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	0%	0%	0%			➤												
		Welded Contacts	Welded Contacts	Welded Contacts	0%	0%	0%			➤												
			Individual welded contacts	Individual welded contacts	0%	0%	0%			➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	0%	0%	0%					➤		➤								
			Drift	Drift & Oscillation	0%	0%	0%					➤		➤								
				Power Spikes	0%	0%	0%					➤		➤								
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	30%	30%	30%	Y								➤	Y	➤		➤	Y	PCc_H2_VALVE
				Incorrect action	40%	40%	40%	Y								➤	Y	➤		➤	Y	PCc_H2_VALVE
				Delayed Action	30%	30%	30%	Y								➤	Y	➤		➤	Y	PCc_H2_VALVE
										0.00%		0.00%		0.00%		60%		0%		99%		

Table 176: FCCS - Actuator 8

Reference	1)A8	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			71.70%	Low	71.28%	Low	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
										Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																		
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	0%	0%	0%			➤												
		Welded Contacts	Welded Contacts	Welded Contacts	0%	0%	0%			➤												
			Individual welded contacts	Individual welded contacts	0%	0%	0%			➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	0%	0%	0%					➤		➤								
			Drift	Drift & Oscillation	0%	0%	0%					➤		➤								
				Power Spikes	0%	0%	0%					➤		➤								
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	30%	30%	30%	Y								➤	Y	➤		➤	Y	PCc_STACK's'_PURGE_VALVE
				Incorrect action	40%	24%	24%	Y								➤	Y	➤		➤		PCc_STACK's'_PURGE_VALVE
				Delayed Action	30%	18%	18%	Y								➤	Y	➤		➤		PCc_STACK's'_PURGE_VALVE
										0.00%		0.00%		0.00%		60%		0%		30%		

Table 177: FCCS - Actuator 9

Reference	1)A9	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		71.70%	Low	71.28%	Low	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
									Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																	
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	0%	0%	0%		➤												
		Welded Contacts	Welded Contacts	Welded Contacts	0%	0%	0%		➤												
			Individual welded contacts	Individual welded contacts	0%	0%	0%		➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	0%	0%	0%				➤		➤								
			Drift	Drift & Oscillation	0%	0%	0%				➤		➤								
				Power Spikes	0%	0%	0%				➤		➤								
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	30%	30%	30%	Y							➤	Y	➤		➤	Y	PCc_DILUTION
				Incorrect action	40%	24%	24%	Y							➤	Y	➤		➤		PCc_DILUTION
				Delayed Action	30%	18%	18%	Y							➤	Y	➤		➤		PCc_DILUTION
									0.00%		0.00%		0.00%		60%		0%		30%		

Table 178: FCCS - Actuator 10

Reference	1)A10	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		99.00%	High	98.85%	Medium	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
									Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																	
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	0%	0%	0%		➤												
		Welded Contacts	Welded Contacts	Welded Contacts	0%	0%	0%		➤												
			Individual welded contacts	Individual welded contacts	0%	0%	0%		➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y			➤		➤	y							PCc_PSU_Mon
			Drift	Drift & Oscillation	15%	15%	15%	Y			➤		➤	y							PCc_PSU_Mon
				Power Spikes	5%	5%	5%	Y			➤		➤	y							PCc_PSU_Mon
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	20%	20%	20%	Y							➤	Y	➤		➤	Y	PCc_PRECHG
				Incorrect action	30%	30%	30%	Y							➤	Y	➤		➤	Y	PCc_PRECHG
				Delayed Action	20%	20%	20%	Y							➤	Y	➤		➤	Y	PCc_PRECHG
									0.00%		0.00%		29.70%		42%		0%		69%		

Table 179: FCCS - Actuator 12

Reference	1)A12	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		71.70%	Low	71.13%	Low	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring		
									Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used	
		Low 60%	Medium 90%	High 99%																	
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	0%	0%	0%		➤												
		Welded Contacts	Welded Contacts	Welded Contacts	0%	0%	0%		➤												
			Individual welded contacts	Individual welded contacts	0%	0%	0%		➤												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y			➤		➤	Y							PCc_PSU_Mon
			Drift	Drift & Oscillation	15%	15%	15%	Y			➤		➤	Y							PCc_PSU_Mon
				Power Spikes	5%	5%	5%	Y			➤		➤	Y							PCc_PSU_Mon
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	20%	12%	12%	Y							➤	Y	➤		➤		PCc_INLET's'_POSITION
				Incorrect action	30%	18%	18%	Y							➤	Y	➤		➤		PCc_INLET's'_POSITION
				Delayed Action	20%	12%	12%	Y							➤	Y	➤		➤		PCc_INLET's'_POSITION
									0.00%		0.00%		29.70%		42%		0%		0%		

Table 180: FCCS - Actuator 13

Reference	1)A13	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		71.70%	Low	71.13%	Low	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring		Voltage or current control (input)		Voltage or current control (output)		Failure Detection by on-line monitoring		Test Pattern		Monitoring	
									Low 60%		Low 60%		High 99%		Low 60%		High 99%		High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.8.1	Used	D.2.8.2	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.11.1	Used
		Low 60%	Medium 90%	High 99%																
Outputs - relays	D.3	Does not energise or de-energise	Does not energise or de-energise	Does not energise or de-energise	0%	0%	0%		➤											
		Welded Contacts	Welded Contacts	Welded Contacts	0%	0%	0%		➤											
			Individual welded contacts	Individual welded contacts	0%	0%	0%		➤											
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y			➤		➤	Y						
			Drift	Drift & Oscillation	15%	15%	15%	Y			➤		➤	Y						
				Power Spikes	5%	5%	5%	Y			➤		➤	Y						
Final Elements	D.12	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	No generic Fault Model available. Detailed Analysis necessary	20%	12%	12%	Y							➤	Y	➤		➤	
				Incorrect action	30%	18%	18%	Y							➤	Y	➤		➤	
				Delayed Action	20%	12%	12%	Y							➤	Y	➤		➤	
									0.00%		0.00%		29.70%		42%		0%		0%	

Table 181: FCCS - Connection 1

Reference	1)C1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
		100%			48.00%	Limited	48.00%	Limited	100.00%	Technique		
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	12%	12%	Y		➤	Y	PCc_OA_WINDOW
				Contact resistance	10%	6%	6%	Y		➤	Y	PCc_OA_WINDOW
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	18%	18%	Y		➤	Y	PCc_OA_WINDOW
			Short Circuit to Vbat	Short Circuit to Vbat	20%	12%	12%	Y		➤	Y	PCc_OA_WINDOW
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y		➤		
				Resistive drift between pins / signal lines	10%	0%	0%	Y		➤		
										79.20%		

Table 182: FCCS - Connection 4

Reference	1)C4	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low	Medium	High								
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	0%	0%	Y		➤		
				Contact resistance	10%	0%	0%	Y		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	0%	0%	Y		➤	Y	PCc_HVNEG
			Short Circuit to Vbat	Short Circuit to Vbat	20%	0%	0%	Y		➤	Y	PCc_HVNEG
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y		➤	Y	PCc_HVNEG
				Resistive drift between pins / signal lines	10%	0%	0%	Y		➤		
										69.30%		

Table 183: FCCS - Connection 5

Reference	1)C5	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			0.00%	Limited	0.00%	Limited	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low	Medium	High								
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	0%	0%	Y		➤		
				Contact resistance	10%	0%	0%	Y		➤	Y	
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	0%	0%	Y		➤	Y	PCc_HVPOS
			Short Circuit to Vbat	Short Circuit to Vbat	20%	0%	0%	Y		➤	Y	PCc_HVPOS
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y		➤	Y	PCc_HVPOS
				Resistive drift between pins / signal lines	10%	0%	0%	Y		➤		
										69.30%		

Table 184: FCCS - Connection 6

Reference	1)C6	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			99.00%	High	99.00%	High	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low	Medium	High								
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	20%	20%	Y		➤	Y	PCc_FAN's'_POWER
				Contact resistance	10%	10%	10%	Y		➤	Y	PCc_FAN's'_POWER
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	30%	30%	Y		➤	Y	PCc_FAN's'_POWER
			Short Circuit to Vbat	Short Circuit to Vbat	20%	20%	20%	Y		➤	Y	PCc_FAN's'_POWER
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y		➤	Y	PCc_FAN's'_POWER
				Resistive drift between pins / signal lines	10%	10%	10%	Y		➤	Y	PCc_FAN's'_POWER
										99.00%		

Table 185: FCCS - Connection 7

Reference	1)C7	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			99.00%	High	99.00%	High	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low	Medium	High								
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	20%	20%	Y		➤	Y	PCc_FAN's'_SPEED
				Contact resistance	10%	10%	10%	Y		➤	Y	PCc_FAN's'_SPEED
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	30%	30%	Y		➤	Y	PCc_FAN's'_SPEED
			Short Circuit to Vbat	Short Circuit to Vbat	20%	20%	20%	Y		➤	Y	PCc_FAN's'_SPEED
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y		➤	Y	PCc_FAN's'_SPEED
				Resistive drift between pins / signal lines	10%	10%	10%	Y		➤	Y	PCc_FAN's'_SPEED
										99.00%		

Table 186: FCCS - Connection 9

Reference	1)C9	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			81.00%	Low	81.00%	Low	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		High 99%		
		Low	Medium	High						D.2.1.1	Used	
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	18%	18%	Y		➤	Y	PCc_STACK's'_TEMP
				Contact resistance	10%	9%	9%	Y		➤	Y	PCc_STACK's'_TEMP
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	27%	27%	Y		➤	Y	PCc_STACK's'_TEMP
			Short Circuit to Vbat	Short Circuit to Vbat	20%	18%	18%	Y		➤	Y	PCc_STACK's'_TEMP
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	9%	9%	Y		➤	Y	PCc_STACK's'_TEMP
				Resistive drift between pins / signal lines	10%	0%	0%	Y		➤		
										89.10%		

Table 187: FCCS - Connection 12

Reference	1)C12	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			42.00%	Limited	42.00%	Limited	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		High 99%		
		Low	Medium	High						D.2.1.1	Used	
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	12%	12%	Y		➤	Y	PCc_H2_VALVE
				Contact resistance	10%	0%	0%	Y		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	18%	18%	Y		➤	Y	PCc_H2_VALVE
			Short Circuit to Vbat	Short Circuit to Vbat	20%	12%	12%	Y		➤	Y	PCc_H2_VALVE
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y		➤		
				Resistive drift between pins / signal lines	10%	0%	0%	Y		➤		
										69.30%		

Table 188: FCCS - Connection 13

Reference	1)C13	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			33.00%	Limited	33.00%	Limited	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		High 99%		
		Low	Medium	High						D.2.1.1	Used	
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	30%	18%	18%	Y		➤	Y	PCc_H2_VALVE
				Contact resistance	15%	0%	0%	Y		➤		
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	0%	0%	0%			➤		
			Short Circuit to Vbat	Short Circuit to Vbat	25%	15%	15%	Y		➤	Y	PCc_H2_VALVE
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	15%	0%	0%	Y		➤		
				Resistive drift between pins / signal lines	15%	0%	0%	Y		➤		
										54.45%		

Table 189: FCCS - Connection 14

Reference	1)C14	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			48.00%	Limited	48.00%	Limited	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		High 99%		
		Low	Medium	High						D.2.1.1	Used	
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	12%	12%	Y		➤	Y	PCc_STACK's'_PURGE_VALVE
				Contact resistance	10%	6%	6%	Y		➤	Y	PCc_STACK's'_PURGE_VALVE
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	18%	18%	Y		➤	Y	PCc_STACK's'_PURGE_VALVE
			Short Circuit to Vbat	Short Circuit to Vbat	20%	12%	12%	Y		➤	Y	PCc_STACK's'_PURGE_VALVE
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y		➤		
				Resistive drift between pins / signal lines	10%	0%	0%	Y		➤		
										79.20%		

Table 190: FCCS - Connection 15

Reference	1)C15	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			42.00%	Limited	42.00%	Limited	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low	Medium	High								
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	30%	18%	18%	Y		➤	Y	PCc_STACK's'_PURGE_VALVE
				Contact resistance	15%	9%	9%	Y		➤	Y	PCc_STACK's'_PURGE_VALVE
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	0%	0%	0%			➤		
			Short Circuit to Vbat	Short Circuit to Vbat	25%	15%	15%	Y		➤	Y	PCc_STACK's'_PURGE_VALVE
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	15%	0%	0%	Y		➤		
				Resistive drift between pins / signal lines	15%	0%	0%	Y		➤		
										69.30%		

Table 191: FCCS - Connection 20

Reference	1)C20	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			48.00%	Limited	48.00%	Limited	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low	Medium	High								
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	12%	12%	Y		➤	Y	PCc_DILUTION
				Contact resistance	10%	6%	6%	Y		➤	Y	PCc_DILUTION
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	18%	18%	Y		➤	Y	
			Short Circuit to Vbat	Short Circuit to Vbat	20%	12%	12%	Y		➤	Y	PCc_DILUTION
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y		➤		
				Resistive drift between pins / signal lines	10%	0%	0%	Y		➤		
										79.20%		

Table 192: FCCS - Connection 22

Reference	1)C22	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			99.00%	High	99.00%	High	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low	Medium	High								
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	20%	20%	Y		➤	Y	PCc_DILUTION
				Contact resistance	10%	10%	10%	Y		➤	Y	PCc_DILUTION
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	30%	30%	Y		➤	Y	PCc_DILUTION
			Short Circuit to Vbat	Short Circuit to Vbat	20%	20%	20%	Y		➤	Y	PCc_DILUTION
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y		➤	Y	PCc_DILUTION
				Resistive drift between pins / signal lines	10%	10%	10%	Y		➤	Y	PCc_DILUTION
										99.00%		

Table 193: FCCS - Connection 24

Reference	1)C24	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			99.00%	High	99.00%	High	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
										High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	
		Low	Medium	High								
		60%	90%	99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	20%	20%	Y		➤	Y	PCc_V_SUM, PCc_HV_WINDOW
				Contact resistance	10%	10%	10%	Y		➤	Y	PCc_V_SUM, PCc_HV_WINDOW
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	30%	30%	Y		➤	Y	PCc_V_SUM, PCc_HV_WINDOW
			Short Circuit to Vbat	Short Circuit to Vbat	20%	20%	20%	Y		➤	Y	PCc_V_SUM, PCc_HV_WINDOW
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y		➤	Y	PCc_V_SUM, PCc_HV_WINDOW
				Resistive drift between pins / signal lines	10%	10%	10%	Y		➤	Y	PCc_V_SUM, PCc_HV_WINDOW
										99.00%		

FCCS - Connection 25

Similar techniques as Connection 24 so not shown.

Table 194: FCCS - Connection 26

Reference	1)C26	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			99.00%	High	99.00%	High	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		High 99% D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	20%	20%	Y		➤	Y	PCc_HVPOS
				Contact resistance	10%	10%	10%	Y		➤	Y	PCc_HVPOS
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	30%	30%	Y		➤	Y	PCc_HVPOS
			Short Circuit to Vbat	Short Circuit to Vbat	20%	20%	20%	Y		➤	Y	PCc_HVPOS
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y		➤	Y	PCc_HVPOS
				Resistive drift between pins / signal lines	10%	10%	10%	Y		➤	Y	PCc_HVPOS
										99.00%		

Table 195: FCCS - Connection 30

Reference	1)C30	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description		Specific PCC
Table 26262-5: 2011		100%			48.00%	Limited	48.00%	Limited	100.00%	Technique		
		Maintain Power - Existing Design								Failure Detection by on-line monitoring		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		High 99% D.2.1.1	Used	
		Low 60%	Medium 90%	High 99%								
Harness including splice and connectors	D.3	Open Circuit	Open Circuit	Open Circuit	20%	12%	12%	Y		➤	Y	PCc_DILUTION
				Contact resistance	10%	6%	6%	Y		➤	Y	PCc_DILUTION
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	30%	18%	18%	Y		➤	Y	
			Short Circuit to Vbat	Short Circuit to Vbat	20%	12%	12%	Y		➤	Y	PCc_DILUTION
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y		➤		
				Resistive drift between pins / signal lines	10%	0%	0%	Y		➤		
										79.20%		

Table 196: FCCS - Data 1 (subset 1)

Reference	1)D1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%		93.60%	Medium	90.79%	Medium	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		
									High 99%		High 99%		High 99%		Low 60%		High 99%		Medium 90%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	
		Low 60%	Medium 90%	High 99%																	
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range		0%	0%		➤		➤		➤		➤		➤		➤		
			Offsets	Offsets		0%	0%		➤		➤		➤				➤		➤		
		Stuck in range	Stuck in range	Stuck in range		0%	0%		➤		➤		➤				➤		➤		
				Oscillation		0%	0%		➤		➤		➤				➤		➤		
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	25%	25%	24%	Y													PCc_DATA_CHECK, PCc_POLL_RESPONSE
		Message corruption	Message corruption	Message corruption	15%	15%	14%	Y													PCc_DATA_CHECK, PCc_POLL_RESPONSE
		Message Delay	Message Delay	Message Delay	20%	18%	17%	Y													PCc_POLL_RESPONSE
		Message Loss	Message Loss	Message Loss	15%	14%	13%	Y													PCc_POLL_RESPONSE
		Unintended message repetition	Unintended message repetition	Unintended message repetition	10%	9%	9%	Y													PCc_POLL_RESPONSE
			Resequencing	Resequencing	5%	5%	4%	Y													PCc_POLL_RESPONSE
			Insertion of message	Insertion of message	5%	5%	4%	Y													PCc_POLL_RESPONSE
				Masquerading	5%	5%	4%	Y													PCc_POLL_RESPONSE
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		

Table 197: FCCS - Data 1 (subset 2)

Reference	1)D1	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description																		Specific PCC
		100%		93.60%	Medium	90.79%	Medium	100.00%	Technique from ISO26262																		
Table 26262-5: 2011		Maintain Power - Existing Design							Sensor ration ality Check		One-bit hardware redundancy		Multi-bit hardware redundancy		Read back of sent message		Complete hardware redundancy		Inspection using test patterns		Transmission redundancy		Information redundancy		Frame counter		Timeout monitoring		Combination of information Redundancy,f rame count and timeout		
									Mixed Low 60%		Low 60%		Medium 90%		Medium 90%		High 99%		High 99%		Medium 90%		Medium 90%		Medium 90%		Medium 90%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	Used		D.2.7.1	Used	D.2.7.2	Used	D.2.7.9	Used	D.2.7.3	Used	D.2.7.4	Used	D.2.7.5	Used	D.2.7.6	Used	D.2.7.7	Used	D.2.7.8	Used	D.2.7.6,7,8	Used	
		Low 60%	Medium 90%	High 99%																										
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range		0%	0%																							
			Offsets	Offsets		0%	0%																							
		Stuck in range	Stuck in range	Stuck in range		0%	0%																							
				Oscillation		0%	0%																							
Data Transmission	D.8	Failure of communication peer	Failure of communication peer	Failure of communication peer	25%	25%	24%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE
		Message corruption	Message corruption	Message corruption	15%	15%	14%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤		➤	Y	PCc_DATA_CHECK, PCc_POLL_RESPONSE
		Message Delay	Message Delay	Message Delay	20%	18%	17%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤	Y	➤		PCc_POLL_RESPONSE
		Message Loss	Message Loss	Message Loss	15%	14%	13%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤	Y	➤		PCc_POLL_RESPONSE
		Unintended message repetition	Unintended message repetition	Unintended message repetition	10%	9%	9%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤	Y	➤		PCc_POLL_RESPONSE
			Resequencing	Resequencing	5%	5%	4%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤	Y	➤		PCc_POLL_RESPONSE
			Insertion of message	Insertion of message	5%	5%	4%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤	Y	➤		PCc_POLL_RESPONSE
				Masquerading	5%	5%	4%	Y		➤		➤		➤		➤		➤		➤		➤		➤		➤	Y	➤		PCc_POLL_RESPONSE
									####		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		54.00%		39.60%		

FCCS - Data 3 to FCCS - Data 38

Similar techniques as Data 1 so not shown.

Table 198: FCCS - Measurement 1

Reference	1)M1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description							Specific PCC
		100%			35.29%	Limited	34.94%	Limited	85.00%	Technique from ISO26262							
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	
										High 99%	Low 60%	High 99%	Medium 90%	High 99%	High 99%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim		Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	
		Low 60%	Medium 90%	High 99%																			
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	15%	0%	0%			➤														
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	10%	6%	6%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_OA_WINDOW
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	9%	9%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_OA_WINDOW
			Short Circuit to Vbat	Short Circuit to Vbat	10%	6%	6%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_OA_WINDOW
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%		Y			➤		➤		➤		➤		➤		➤		
			Offsets	Offsets	15%	0%	0%		Y			➤		➤		➤		➤		➤		➤		
		Stuck in range	Stuck in range	Stuck in range	15%	9%	9%		Y			➤		➤		➤		➤		➤		➤		
			Drift & Oscillation	Drift & Oscillation	10%	0%	0%		Y			➤		➤		➤		➤		➤		➤		
										0.00%		30.00%		0.00%		0.00%		0.00%		49.50%		0.00%		

Table 199: FCCS - Measurement 2

Reference	1)M2	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description							Specific PCC
		100%			99.00%	High	98.01%	Medium	100.00%	Technique from ISO26262							
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	
										High 99%	Low 60%	High 99%	Medium 90%	High 99%	High 99%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim		Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	
		Low 60%	Medium 90%	High 99%																			
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	0%	0%	0%			➤														
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	15%	15%	15%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_V_SUM, PCc_HV_WINDOW
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	20%	20%	20%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_V_SUM, PCc_HV_WINDOW
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_V_SUM, PCc_HV_WINDOW
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_V_SUM, PCc_HV_WINDOW
			Offsets	Offsets	15%	15%	15%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_V_SUM, PCc_HV_WINDOW
		Stuck in range	Stuck in range	Stuck in range	20%	20%	20%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_V_SUM, PCc_HV_WINDOW
			Drift & Oscillation	Drift & Oscillation	10%	10%	10%		Y			➤	Y	➤		➤		➤		➤	Y	➤		
										0.00%		60.00%		0.00%		0.00%		0.00%		99.00%		0.00%		

FCCS – Measurement 3

Similar techniques as measurement 2 so not shown.

Table 200: FCCS - Measurement 4

Reference	1)M4	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description							
		100%		99.00%	High	98.01%	Medium	100.00%	Technique from ISO26262							
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Specific PCC
									High 99%	Low 60%	High 99%	Medium 90%	High 99%	High 99%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1 Used	D.2.1.1 Used	D.2.6.1 Used	D.2.6.2 Used	D.2.6.3 Used	D.2.6.4 Used	D.2.6.5 Used	
		Low 60%	Medium 90%	High 99%												
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	0%	0%	0%									
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	15%	15%	15%	Y		Y						PCc_HVPOS
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	20%	20%	20%	Y		Y						PCc_HVPOS
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	Y		Y						PCc_HVPOS
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y		Y						PCc_HVPOS
			Offsets	Offsets	15%	15%	15%	Y		Y						PCc_HVPOS
		Stuck in range	Stuck in range	Stuck in range	20%	20%	20%	Y		Y						PCc_HVPOS
			Drift & Oscillation	Drift & Oscillation	10%	10%	10%	Y		Y						PCc_HVPOS
									0.00%	60.00%	0.00%	0.00%	0.00%	99.00%	0.00%	

Table 201: FCCS - Measurement 7

Reference	1)M7	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description							
		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262							
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring	Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Specific PCC
									High 99%	Low 60%	High 99%	Medium 90%	High 99%	High 99%	High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1 Used	D.2.1.1 Used	D.2.6.1 Used	D.2.6.2 Used	D.2.6.3 Used	D.2.6.4 Used	D.2.6.5 Used	
		Low 60%	Medium 90%	High 99%												
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	0%	0%	0%									
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	15%	0%	0%	Y								
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	20%	0%	0%	Y								
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	Y								
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y								
			Offsets	Offsets	15%	0%	0%	Y								
		Stuck in range	Stuck in range	Stuck in range	20%	0%	0%	Y								
			Drift & Oscillation	Drift & Oscillation	10%	0%	0%	Y								
									0.00%	0.00%	44.55%	0.00%	0.00%	0.00%	0.00%	

Table 202: FCCS - Measurement 18

Reference	1)M18	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%			99.00%	High	98.01%	Medium	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		
										High		Low		High		Medium		High		High		High	
										99%		60%		99%		90%		99%		99%		99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim		Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	
		Low	Medium	High																				
		60%	90%	99%																				
Harness including splice and connectors	D.3			Resistive drift between pins / signal lines	0%	0%	0%			➤														
Analogue and digital Inputs	D.7	Open circuit	Open circuit	Open circuit	15%	15%	15%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_A_SUM
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	20%	20%	20%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_A_SUM
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_A_SUM
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_A_SUM
			Offsets	Offsets	15%	15%	15%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_A_SUM
		Stuck in range	Stuck in range	Stuck in range	20%	20%	20%		Y			➤	Y	➤		➤		➤		➤	Y	➤		PCc_A_SUM
			Drift & Oscillation	Drift & Oscillation	10%	10%	10%		Y			➤	Y	➤		➤		➤		➤	y	➤		PCc_A_SUM
										0.00%		60.00%		0.00%		0.00%		0.00%		99.00%		0.00%	

FCCS – Measurement 19

Similar techniques as measurement 18 so not shown.

Table 203: FCCS - Output 1

Reference	1)O1	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%			99.00%	High	98.18%	Medium	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)	
										Low		High		Medium		High		High		High		Low		High	
										60%		99%		90%		99%		99%		99%		60%		99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim		Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																						
		60%	90%	99%																						
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%	20%	20%		Y	➤	Y	➤		➤		➤		➤	Y	➤						PCc_HVNEG
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	20%	20%	20%		Y	➤	Y	➤		➤		➤		➤	Y	➤						PCc_HVNEG
			Short Circuit to Vbat	Short Circuit to Vbat	15%	15%	15%		Y	➤	Y	➤		➤		➤		➤	Y	➤						PCc_HVNEG
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%		Y	➤	Y	➤		➤		➤		➤	Y	➤						PCc_HVNEG
			Offsets	Offsets		0%	0%			➤		➤		➤		➤		➤		➤						
		Stuck in range	Stuck in range	Stuck in range		0%	0%			➤		➤		➤		➤		➤		➤						
				Drift & Oscillation		0%	0%			➤		➤		➤		➤		➤		➤						
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%		y													➤		➤	Y	PCc_PSU
			Drift	Drift & Oscillation	20%	20%	20%		y													➤		➤	Y	PCc_PSU
				Power Spikes	5%	5%	5%		y													➤		➤	Y	PCc_PSU
										39.00%		0.00%		0.00%		0.00%		64.35%		0.00%		0.00%		34.65%	

Table 204: FCCS - Output 2

Reference	1)O2	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%			99.00%	High	98.18%	Medium	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)	
										Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		Low 60%		High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution		Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																						
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%		20%	20%	Y		Y								Y							PCc_HVPOS
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	20%		20%	20%	Y		Y								Y							PCc_HVPOS
			Short Circuit to Vbat	Short Circuit to Vbat	15%		15%	15%	Y		Y								Y							PCc_HVPOS
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%		10%	10%	Y		Y								Y							PCc_HVPOS
			Offsets	Offsets			0%	0%																		
		Stuck in range	Stuck in range	Stuck in range			0%	0%																		
				Drift & Oscillation			0%	0%																		
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%		10%	10%	y															Y		PCc_PSU
			Drift	Drift & Oscillation	20%		20%	20%	y															Y		PCc_PSU
				Power Spikes	5%		5%	5%	y															Y		PCc_PSU

Table 205: FCCS - Output 6

Reference	1)O6	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Specific PCC
		100%			99.00%	High	98.18%	Medium	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1								Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)	
										Low 60%		High 99%		Medium 90%		High 99%		High 99%		High 99%		Low 60%		High 99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution		Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low 60%	Medium 90%	High 99%																						
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%		20%	20%	Y		Y								Y							PCc_FAN's'_POWER
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%		15%	15%	Y		Y								Y							PCc_FAN's'_POWER
			Short Circuit to Vbat	Short Circuit to Vbat	10%		10%	10%	Y		Y								Y							PCc_FAN's'_POWER
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%		10%	10%	Y		Y								Y							PCc_FAN's'_POWER
			Offsets	Offsets			0%	0%																		
		Stuck in range	Stuck in range	Stuck in range	10%		10%	10%	Y		Y								Y							PCc_FAN's'_POWER
				Drift & Oscillation			0%	0%																		
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%		10%	10%	Y															Y		PCc_PSU
			Drift	Drift & Oscillation	20%		20%	20%	Y															Y		PCc_PSU
				Power Spikes	5%		5%	5%	Y															Y		PCc_PSU
										39.00%		0.00%		0.00%		0.00%		64.35%		0.00%		0.00%		34.65%	

Table 206: FCCS - Output 7

Reference	1)O7	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%			99.00%	High	98.18%	Medium	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Cells in Operating Area Architecture Candidate 1								Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		
										Low		High		Medium		High		High		High		Low		High		
										60%		99%		90%		99%		99%		99%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																						
		60%	90%	99%																						
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%	20%	20%	Y			Y								Y							PCc_FAN's'_SPEED
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	15%	15%	Y			Y								Y							PCc_FAN's'_SPEED
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	Y			Y								Y							PCc_FAN's'_SPEED
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y			Y								Y							PCc_FAN's'_SPEED
			Offsets	Offsets		0%	0%																			
		Stuck in range	Stuck in range	Stuck in range	10%	10%	10%	Y			Y								Y							PCc_FAN's'_SPEED
				Drift & Oscillation		0%	0%																			
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y																Y		PCc_PSU
			Drift	Drift & Oscillation	20%	20%	20%	Y																Y		PCc_PSU
				Power Spikes	5%	5%	5%	Y																Y		PCc_PSU
										39.00%		0.00%		0.00%		0.00%		64.35%		0.00%		0.00%		34.65%		

Table 207: FCCS - Output 10

Reference	1)O10	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%			99.00%	High	98.18%	Medium	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Power - Existing Design								Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		
										Low		High		Medium		High		High		High		Low		High		
										60%		99%		90%		99%		99%		99%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																						
		60%	90%	99%																						
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%	20%	20%	Y			Y								Y							PCc_H2_VALVE
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	15%	15%	Y			Y								Y							PCc_H2_VALVE
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	Y			Y								Y							PCc_H2_VALVE
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y			Y								Y							PCc_H2_VALVE
			Offsets	Offsets		0%	0%																			
		Stuck in range	Stuck in range	Stuck in range	10%	10%	10%	Y			Y								Y							
				Drift & Oscillation		0%	0%																			
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y																Y		PCc_PSU
			Drift	Drift & Oscillation	20%	20%	20%	Y																Y		PCc_PSU
				Power Spikes	5%	5%	5%	Y																Y		PCc_PSU
										39.00%		0.00%		0.00%		0.00%		64.35%		0.00%		0.00%		34.65%		

Table 208: FCCS - Output 11

Reference	1)O11	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		
									Low		High		Medium		High		High		High		Low		High		
									60%		99%		90%		99%		99%		99%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																					
		60%	90%	99%																					
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%	0%	0%	Y	➤		➤		➤		➤		➤		➤						
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%	Y	➤		➤		➤		➤		➤		➤						
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	Y	➤		➤		➤		➤		➤		➤						
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y	➤		➤		➤		➤		➤		➤						
			Offsets	Offsets		0%	0%		➤		➤		➤		➤		➤		➤						
		Stuck in range	Stuck in range	Stuck in range	10%	0%	0%	Y	➤		➤		➤		➤		➤		➤						
				Drift & Oscillation		0%	0%		➤		➤		➤		➤		➤		➤						
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	Y													➤		➤	Y	PCc_PSU
			Drift	Drift & Oscillation	20%	0%	0%	Y													➤		➤	Y	PCc_PSU
				Power Spikes	5%	0%	0%	Y													➤		➤	Y	PCc_PSU
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		34.65%		

Table 209: FCCS - Output 12

Reference	1)O12	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%		99.00%	High	98.18%	Medium	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)		Voltage or current control (output)		
									Low		High		Medium		High		High		High		Low		High		
									60%		99%		90%		99%		99%		99%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																					
		60%	90%	99%																					
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%	20%	20%	Y	➤	Y	➤		➤		➤		➤	Y	➤						PCc_STACK's'_PURGE_VALVE
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	15%	15%	Y	➤	Y	➤		➤		➤		➤	Y	➤						PCc_STACK's'_PURGE_VALVE
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	Y	➤	Y	➤		➤		➤		➤	Y	➤						PCc_STACK's'_PURGE_VALVE
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y	➤	Y	➤		➤		➤		➤	Y	➤						PCc_STACK's'_PURGE_VALVE
			Offsets	Offsets		0%	0%		➤		➤		➤		➤		➤		➤						
		Stuck in range	Stuck in range	Stuck in range	10%	10%	10%	Y	➤	Y	➤		➤		➤		➤	Y	➤						PCc_STACK's'_PURGE_VALVE
				Drift & Oscillation		0%	0%		➤		➤		➤		➤		➤		➤						
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y													➤		➤	Y	PCc_PSU
			Drift	Drift & Oscillation	20%	20%	20%	Y													➤		➤	Y	PCc_PSU
				Power Spikes	5%	5%	5%	Y													➤		➤	Y	PCc_PSU
									39.00%		0.00%		0.00%		0.00%		64.35%		0.00%		0.00%		34.65%		

Table 210: FCCS - Output 13

Reference	1)O13	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Voltage or current control (input)	Voltage or current control (output)	
									Low	High	Medium	High	High	High	Low	High	
									60%	99%	90%	99%	99%	99%	60%	99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																					
		60%	90%	99%																					
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%	0%	0%	Y																	
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%	Y																	
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	Y																	
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y																	
			Offsets	Offsets		0%	0%																		
		Stuck in range	Stuck in range	Stuck in range	10%	0%	0%	Y																	
				Drift & Oscillation		0%	0%																		
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	Y																	PCc_PSU
			Drift	Drift & Oscillation	20%	0%	0%	Y																	PCc_PSU
				Power Spikes	5%	0%	0%	Y																	PCc_PSU
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		34.65%		

Table 211: FCCS - Output 16

Reference	1)O16	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description								Specific PCC
		100%		99.00%	High	98.18%	Medium	100.00%	Technique from ISO26262								
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring	Test Pattern	Code protection	Multi-channel parallel output	Monitored outputs	Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.	Voltage or current control (input)	Voltage or current control (output)	
									Low	High	Medium	High	High	High	Low	High	
									60%	99%	90%	99%	99%	99%	60%	99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																					
		60%	90%	99%																					
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%	20%	20%	Y		Y								Y							PCc_DILUTION
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	15%	15%	Y		Y								Y							PCc_DILUTION
			Short Circuit to Vbat	Short Circuit to Vbat	10%	10%	10%	Y		Y								Y							PCc_DILUTION
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y		Y								Y							PCc_DILUTION
			Offsets	Offsets		0%	0%																		
		Stuck in range	Stuck in range	Stuck in range	10%	10%	10%	Y		Y								Y							PCc_DILUTION
				Drift & Oscillation		0%	0%																		
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y																	PCc_PSU
			Drift	Drift & Oscillation	20%	20%	20%	Y																	PCc_PSU
				Power Spikes	5%	5%	5%	Y																	PCc_PSU
									39.00%		0.00%		0.00%		0.00%		64.35%		0.00%		34.65%		

Table 212: FCCS - Output 17

Reference	1)O17	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description												
		100%		99.00%	High	98.18%	Medium	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)	Voltage or current control (output)	Specific PCC
									Low		High		Medium		High		High		High		Low	High	
									60%		99%		90%		99%		99%		99%		60%	99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1 Used	D.2.8.2 Used	
		Low	Medium	High																			
		60%	90%	99%																			
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%	20%	20%	Y	➤	Y	➤		➤		➤		➤	Y	➤				PCc_PRECHG
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	20%	20%	20%	Y	➤	Y	➤		➤		➤		➤	Y	➤				PCc_PRECHG
			Short Circuit to Vbat	Short Circuit to Vbat	15%	15%	15%	Y	➤	Y	➤		➤		➤		➤	Y	➤				PCc_PRECHG
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	10%	10%	Y	➤	Y	➤		➤		➤		➤	Y	➤				PCc_PRECHG
			Offsets	Offsets		0%	0%		➤		➤		➤		➤		➤		➤				
		Stuck in range	Stuck in range	Stuck in range		0%	0%		➤		➤		➤		➤		➤		➤				
				Drift & Oscillation		0%	0%		➤		➤		➤		➤		➤		➤				
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y													➤	➤ Y	PCc_PSU
			Drift	Drift & Oscillation	20%	20%	20%	y													➤	➤ Y	PCc_PSU
				Power Spikes	5%	5%	5%	y													➤	➤ Y	PCc_PSU
									39.00%		0.00%		0.00%		0.00%		64.35%		0.00%		0.00%	34.65%	

Table 213: FCCS - Output 19

Reference	1)O19	Failure Mode Distribution		Full Claim		PCc Claim		SG Failure Distribution	Technique Description												
		100%		0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring		Test Pattern		Code protection		Multi-channel parallel output		Monitored outputs		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Voltage or current control (input)	Voltage or current control (output)	Specific PCC
									Low		High		Medium		High		High		High		Low	High	
									60%		99%		90%		99%		99%		99%		60%	99%	
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.2	Used	D.2.6.3	Used	D.2.6.4	Used	D.2.6.5	Used	D.2.8.1 Used	D.2.8.2 Used	
		Low	Medium	High																			
		60%	90%	99%																			
Analogue and digital Outputs - stuck at	D.7	Open circuit	Open circuit	Open circuit	20%	0%	0%	Y	➤		➤		➤		➤		➤		➤				
		Short Circuit to ground	Short Circuit to ground (dc Coupled)	Short Circuit to ground (dc Coupled)	15%	0%	0%	Y	➤		➤		➤		➤		➤		➤				
			Short Circuit to Vbat	Short Circuit to Vbat	10%	0%	0%	Y	➤		➤		➤		➤		➤		➤				
			Short circuit between neighbouring pins	Short circuit between neighbouring pins	10%	0%	0%	Y	➤		➤		➤		➤		➤		➤				
			Offsets	Offsets		0%	0%		➤		➤		➤		➤		➤		➤				
		Stuck in range	Stuck in range	Stuck in range	10%	0%	0%	Y	➤		➤		➤		➤		➤		➤				
				Drift & Oscillation		0%	0%		➤		➤		➤		➤		➤		➤				
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	Y													➤	➤ Y	PCc_PSU
			Drift	Drift & Oscillation	20%	0%	0%	Y													➤	➤ Y	PCc_PSU
				Power Spikes	5%	0%	0%	Y													➤	➤ Y	PCc_PSU
									0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%	34.65%	

Table 214: FCCS - Parameter 7 (subset 1)

Reference	1)P7	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%			98.55%	Medium	97.49%	Medium	100.00%	Technique from ISO26262										
Table 26262-5: 2011		Maintain Power - Existing Design								Voltage or current control (input)		Voltage or current control (output)		Watchdog with separate time base without time-window		Watchdog with separate time base and time-window		Logical monitoring of program sequence		Combination of temporal and logical monitoring of program sequences		Combination of temporal and logical monitoring of program sequences with time dependency		
										Low		High		Low		Medium		Medium		High		High		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim		Failure Mode Leads to Violation of Safety Goal	60%		99%		60%		90%		90%		99%		99%		
		Low	Medium	High						D.2.8.1	Used	D.2.8.2	Used	D.2.9.1	Used	D.2.9.2	Used	D.2.9.3	Used	D.2.9.4	Used	D.2.9.5	Used	
		60%	90%	99%																				
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	15%	15%	15%		Y				y											PCc_PSU
			Drift	Drift & Oscillation	15%	15%	15%		Y				y											PCc_PSU
				Power Spikes	10%	10%	10%		Y				y											PCc_PSU
Clock	D.10	stuck at	stuck at	stuck at		0%	0%																	
			dc fault model	dc fault model		0%	0%																	
				Incorrect frequency		0%	0%																	
				Period jitter		0%	0%																	
Non-volatile Memory	D.5	stuck at	stuck at	stuck at		0%	0%																	
			dc fault model	dc fault model		0%	0%																	
Volatile Memory	D.6	stuck at	stuck at	stuck at	10%	10%	10%		Y															PCc_RAM_TEST
			dc fault model	dc fault model	10%	10%	10%		Y															PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%		Y															PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	10%	10%	10%		Y															PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	10%	10%	10%		Y															PCc_MICRO_TEST
				dc fault model	10%	10%	10%		Y															PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%		Y															PCc_MICRO_TEST
										0.00%		39.60%		0.00%		0.00%		0.00%		0.00%		0.00%		

Table 215: FCCS - Parameter 7 (subset 2)

Reference	1)P7	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Technique Description										Specific PCC
		100%			98.55%	Medium	97.49%	Medium	100.00%	Technique from ISO26262														Technique from ISO26262										
Table 26262-5: 2011		Maintain Power - Existing Design								Parity bit		Memory monitoring using error-detection-correction codes (EDC)		Modified checksum		Memory signature		Block replication (for example, double memory with hardware or software comparison)		RAM Pattern test		RAM March test		Parity bit		Memory monitoring using error-detection-correction codes (EDC)		Block replication (for example, double memory with hardware or software comparison)		Running checksum/CRC		
										Low		High		Low		High		High		Medium		High		Low		High		High		High		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim		Failure Mode Leads to Violation of Safety Goal	60%		99%		60%		99%		99%		90%		99%		60%		99%		99%		99%		
		Low	Medium	High						D.2.5.2	Used	D.2.4.1	Used	D.2.4.2	Used	D.2.4.3	Used	D.2.4.4	Used	D.2.5.1	Used	D.2.5.3	Used	D.2.5.2	Used	D.2.4.1	Used	D.2.4.4	Used	D.2.5.4	Used	
		60%	90%	99%																												
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	15%	15%	15%		Y																							PCc_PSU
			Drift	Drift & Oscillation	15%	15%	15%		Y																							PCc_PSU
				Power Spikes	10%	10%	10%		Y																							PCc_PSU
Clock	D.10	stuck at	stuck at	stuck at		0%	0%																									
			dc fault model	dc fault model		0%	0%																									
				Incorrect frequency		0%	0%																									
				Period jitter		0%	0%																									
Non-volatile Memory	D.5	stuck at	stuck at	stuck at		0%	0%																									
			dc fault model	dc fault model		0%	0%																									
Volatile Memory	D.6	stuck at	stuck at	stuck at	10%	10%	10%		Y											y												PCc_RAM_TEST
			dc fault model	dc fault model	10%	10%	10%		Y											y												PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%		Y											y												PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	10%	10%	10%		Y																							PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	10%	10%	10%		Y																							PCc_MICRO_TEST
				dc fault model	10%	10%	10%		Y																							PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%		Y																							PCc_MICRO_TEST
										0.00%		0.00%		0.00%		0.00%		0.00%		22.50%		0.00%		0.00%		0.00%		0.00%		24.75%		

Table 216: FCCS - Parameter 7 (subset 3)

Reference	1)P7	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														
		100%			98.55%	Medium	97.49%	Medium	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Maintain Power - Existing Design								Self-test by software		Self-test by software cross exchanged between two independent units		Self-test supported by hardware (one-channel)		Software diversified redundancy (one hardware channel)		Reciprocal comparison by software in separate processing units		HW redundancy (e.g. Dual Core Lockstep, asymmetric redundancy, coded processing)		Configuration register test		Stack over/under flow detection		Integrated hardware consistency monitoring		Self-test by software		Self-test supported by hardware (one-channel)		Specific PCC
										Medium		Medium		Medium		High		High		High		High		Low		High		Medium		High		
										90%		90%		90%		99%		99%		99%		99%		60%		99%		90%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.3.1	Used	D.2.3.3	Used	D.2.3.2	Used	D.2.3.4	Used	D.2.3.5	Used	D.2.3.6	Used	D.2.3.7	Used	D.2.3.8	Used	D.2.3.9	Used	D.2.3.1	Used	D.2.3.2	Used	
		Low	Medium	High																											
		60%	90%	99%																											
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	15%	15%	15%	Y																						PCc_PSU
			Drift	Drift & Oscillation	15%	15%	15%	Y																						PCc_PSU
				Power Spikes	10%	10%	10%	Y																						PCc_PSU
Clock	D.10	stuck at	stuck at	stuck at		0%	0%																								
			dc fault model	dc fault model		0%	0%																								
				Incorrect frequency		0%	0%																								
				Period jitter		0%	0%																								
Non-volatile Memory	D.5	stuck at	stuck at	stuck at		0%	0%																								
			dc fault model	dc fault model		0%	0%																								
Volatile Memory	D.6	stuck at	stuck at	stuck at	10%	10%	10%	Y																						PCc_RAM_TEST
			dc fault model	dc fault model	10%	10%	10%	Y																						PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	Y																						PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	10%	10%	10%	Y			y												y							PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	10%	10%	10%	Y			y												y							PCc_MICRO_TEST
				dc fault model	10%	10%	10%	Y			y												y							PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	Y																				y		PCc_MICRO_TEST
										27%		0%		0%		0%		0%		0%		30%		0%		0%		5%		0%	

Table 217: FCCS - Parameter 57 (subset 1)

Reference	1)P57	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														
		100%			98.55%	Medium	97.54%	Medium	100.00%	Technique from ISO26262														
Table 26262-5: 2011		Maintain Power - Existing Design								Voltage or current control (input)		Voltage or current control (output)		Watchdog with separate time base without time-window		Watchdog with separate time base and time-window		Logical monitoring of program sequence		Combination of temporal and logical monitoring of program sequences		Combination of temporal and logical monitoring of program sequences with time dependency		Specific PCC
										Low		High		Low		Medium		Medium		High		High		
										60%		99%		60%		90%		90%		99%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.8.1	Used	D.2.8.2	Used	D.2.9.1	Used	D.2.9.2	Used	D.2.9.3	Used	D.2.9.4	Used	D.2.9.5	Used	
		Low	Medium	High																				
		60%	90%	99%																				
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y					y											PCc_PSU
			Drift	Drift & Oscillation	10%	10%	10%	Y					y											PCc_PSU
				Power Spikes	10%	10%	10%	Y					y											PCc_PSU
Clock	D.10	stuck at	stuck at	stuck at		0%	0%																	
			dc fault model	dc fault model		0%	0%																	
				Incorrect frequency		0%	0%																	
				Period jitter		0%	0%																	
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	10%	10%	10%	Y																PCc_NV_TEST
			dc fault model	dc fault model	10%	10%	10%	Y																PCc_NV_TEST
Volatile Memory	D.6	stuck at	stuck at	stuck at	10%	10%	10%	Y																PCc_RAM_TEST
			dc fault model	dc fault model	10%	10%	10%	Y																PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	Y																PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	10%	10%	10%	Y																PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	Y																PCc_MICRO_TEST
				dc fault model	5%	5%	5%	Y																PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	Y																PCc_MICRO_TEST
										0.00%		29.70%		0.00%		0.00%		0.00%		0.00%		0.00%		

Table 218: FCCS - Parameter 57 (subset 2)

Reference	1)P57	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description														Technique Description												Specific PCC
		100%			98.55%	Medium	97.54%	Medium	100.00%	Technique from ISO26262														Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design								Parity bit		Memory monitoring using error-detection-correction codes (EDC)		Modified checksum		Memory signature		Block replication (for example, double memory with hardware or software comparison)		RAM Pattern test		RAM March test		Parity bit		Memory monitoring using error-detection-correction codes (EDC)		Block replication (for example, double memory with hardware or software comparison)		Running checksum/CRC			
										Low		High		Low		High		High		Medium		High		Low		High		High		High			
										60%		99%		60%		99%		99%		90%		99%		60%		99%		99%		99%			
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.5.2	Used	D.2.4.1	Used	D.2.4.2	Used	D.2.4.3	Used	D.2.4.4	Used	D.2.5.1	Used	D.2.5.3	Used	D.2.5.2	Used	D.2.4.1	Used	D.2.4.4	Used	D.2.5.4	Used		
		Low	Medium	High																															
		60%	90%	99%																															
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y																											PCc_PSU
			Drift	Drift & Oscillation	10%	10%	10%	Y																											PCc_PSU
				Power Spikes	10%	10%	10%	Y																											PCc_PSU
Clock	D.10	stuck at	stuck at	stuck at		0%	0%																												
			dc fault model	dc fault model		0%	0%																												
				Incorrect frequency		0%	0%																												
				Period jitter		0%	0%																												
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	10%	10%	10%	Y				Y				Y																			PCc_NV_TEST
			dc fault model	dc fault model	10%	10%	10%	Y				Y				Y																			PCc_NV_TEST
Volatile Memory	D.6	stuck at	stuck at	stuck at	10%	10%	10%	Y													y														PCc_RAM_TEST
			dc fault model	dc fault model	10%	10%	10%	Y													y														PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	Y													y														PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	10%	10%	10%	Y																											PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	Y																											PCc_MICRO_TEST
				dc fault model	5%	5%	5%	Y																											PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	Y																											PCc_MICRO_TEST
										0.00%		19.80%		0.00%		19.80%		0.00%		22.50%		0.00%		0.00%		0.00%		0.00%		24.75%			

Table 219: FCCS - Parameter 57 (subset 3)

Reference	1)P57	Failure Mode Distribution			Full Claim		PCc Claim		SG Failure Distribution	Technique Description																										Specific PCC
		100%			98.55%	Medium	97.54%	Medium	100.00%	Technique from ISO26262																										
Table 26262-5: 2011		Maintain Power - Existing Design								Self-test by software		Self-test by software cross exchanged between two independent units		Self-test supported by hardware (one-channel)		Software, diversified, redundancy (one hardware channel)		Reciprocal comparison by software in separate processing units		HW redundancy (e.g. Dual Core Lockstep, asymmetric redundancy, coded processing)		Configuration register test		Stack over/under flow detection		Integrated hardware consistency monitoring		Self-test by software		Self-test supported by hardware (one-channel)			
										Medium		Medium		Medium		High		High		High		High		Low		High		Medium		High			
										90%		90%		90%		99%		99%		99%		99%		60%		99%		90%		99%			
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal		D.2.3.1	Used	D.2.3.1	Used	D.2.3.2	Used	D.2.3.4	Used	D.2.3.5	Used	D.2.3.6	Used	D.2.3.7	Used	D.2.3.8	Used	D.2.3.9	Used	D.2.3.1	Used	D.2.3.2	Used		
		Low	Medium	High																															
		60%	90%	99%																															
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	Y																											PCc_PSU
			Drift	Drift & Oscillation	10%	10%	10%	Y																											PCc_PSU
				Power Spikes	10%	10%	10%	Y																											PCc_PSU
Clock	D.10	stuck at	stuck at	stuck at		0%	0%																												
			dc fault model	dc fault model		0%	0%																												
				Incorrect frequency		0%	0%																												
				Period jitter		0%	0%																												
Non-volatile Memory	D.5	stuck at	stuck at	stuck at	10%	10%	10%	Y																											PCc_NV_TEST
			dc fault model	dc fault model	10%	10%	10%	Y																											PCc_NV_TEST
Volatile Memory	D.6	stuck at	stuck at	stuck at	10%	10%	10%	Y																											PCc_RAM_TEST
			dc fault model	dc fault model	10%	10%	10%	Y																											PCc_RAM_TEST
			soft error model	soft error model	5%	5%	5%	Y																											PCc_RAM_TEST
Processing Units : ALU - Data Path	D.4	Stuck at	Stuck at	Stuck at	10%	10%	10%	Y			y												y		y										PCc_MICRO_TEST
			Stuck at at gate level	Stuck at at gate level	5%	5%	5%	Y			y												y												PCc_MICRO_TEST
				dc fault model	5%	5%	5%	Y			y												y												PCc_MICRO_TEST
Processing Units : ALU - Data Path	D.13			Soft error model for sequential parts	5%	5%	4%	Y																							y				PCc_MICRO_TEST
										18%		0%		0%		0%		0%		0%		20%		0%		0%		5%		0%			

Table 220: FCCS - PSU

Reference	1)PSU	Failure Mode Distribution			Full Claim	PCc Claim	Technique Description				Specific PCC
		100%			99%	99%	1				
Table D.9 26262-5: 2011		Maintain Power - Existing Design					Voltage or current control (input)		Voltage or current control (output)		
							Low 60%		High 99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High								
		60%	90%	99%								
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	50%	50%	49%				y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%				y	PCc_PSU_Mon
				Power Spikes	30%	30%	30%				y	PCc_PSU_Mon
								0.00%		99.00%		

Table 221: FCCS - Transducer 2

Reference	1)T2	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%	0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design						Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Voltage or current control (input)		Voltage or current control (output)		
								High		High		High		Low		High		Medium		Low		High		
								99%		99%		99%		60%		99%		90%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																				
		60%	90%	99%																				
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	0%	0%	y							Y										PCc_STACK's'_TEMP
			Offsets	Offsets	10%	0%	0%	y																	
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y																	
				Oscillation	5%	0%	0%	y																	
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	y															y		PCc_PSU_MON
			Drift	Drift & Oscillation	20%	0%	0%	y															y		PCc_PSU_MON
				Power Spikes	5%	0%	0%	y															y		PCc_PSU_MON
									0.00%		0.00%		0.00%		12.00%		0.00%		0.00%		0.00%		34.65%		

Table 222: FCCS - Transducer 5

Reference	1)T5	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%	0.00%	Limited	0.00%	Limited	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design						Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Voltage or current control (input)		Voltage or current control (output)		
								High		High		High		Low		High		Medium		Low		High		
								99%		99%		99%		60%		99%		90%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																				
		60%	90%	99%																				
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	0%	0%	y							Y										PCc_DILUTION
			Offsets	Offsets	10%	0%	0%	y																	PCc_DILUTION
		Stuck in range	Stuck in range	Stuck in range	30%	0%	0%	y																	
				Oscillation	5%	0%	0%	y		Y															PCc_DILUTION
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	0%	0%	y															y		PCc_PSU_MON
			Drift	Drift & Oscillation	20%	0%	0%	y															y		PCc_PSU_MON
				Power Spikes	5%	0%	0%	y															y		PCc_PSU_MON
									4.95%		0.00%		0.00%		12.00%		0.00%		0.00%		0.00%		34.65%		

Table 223: FCCS - Transducer 7

Reference	1)T7	Failure Mode Distribution	Full Claim		PCc Claim		SG Failure Distribution	Technique Description												Specific PCC
		100%	99.00%	High	97.54%	Medium	100.00%	Technique from ISO26262												
Table 26262-5: 2011		Maintain Power - Existing Design						Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Voltage or current control (input)		Voltage or current control (output)		
								High		High		High		Low		High		Medium		Low		High		
								99%		99%		99%		60%		99%		90%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																				
		60%	90%	99%																				
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	20%	19%	y		Y															PCc_A_SUM
			Offsets	Offsets	10%	10%	10%	y		Y															PCc_A_SUM
		Stuck in range	Stuck in range	Stuck in range	30%	30%	29%	y		Y															PCc_A_SUM
				Oscillation	5%	5%	5%	y		Y															PCc_A_SUM
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y															y		PCc_PSU_MON
			Drift	Drift & Oscillation	20%	20%	20%	y															y		PCc_PSU_MON
				Power Spikes	5%	5%	5%	y															y		PCc_PSU_MON
									64.35%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		34.65%		

Table 224: FCCS - Transducer 8

Reference	1)T8	Failure Mode Distribution			Full Claim	PCc Claim		SG Failure Distribution	Technique Description										Specific PCC
		100%			99.00%	High	97.54%	Medium	100.00%	Technique from ISO26262									
Table 26262-5: 2011		Maintain Power - Existing Design							Failure Detection by on-line monitoring		Test Pattern		Input Comparison Voting (1oo2, 2oo3 or better redundancy). Only if data flow changes within diagnostic test interval.		Sensor valid range		Sensor Correlation		Sensor rationality Check		Voltage or current control (input)		Voltage or current control (output)		
									High		High		High		Low		High		Medium		Low		High		
									99%		99%		99%		60%		99%		90%		60%		99%		
Element	See Table	Analysed Failure modes for low / medium / high Diagnostic Coverage			Failure Mode Distribution	Full Claim	PCc Claim	Failure Mode Leads to Violation of Safety Goal	D.2.1.1	Used	D.2.6.1	Used	D.2.6.5	Used	D.2.10.1	Used	D.2.10.2	Used	D.2.10.3	Used	D.2.8.1	Used	D.2.8.2	Used	
		Low	Medium	High																					
		60%	90%	99%																					
Sensors including Signal Switches	D.11	Out of range	Out of range	Out of range	20%	20%	19%	y	➤	Y	➤		➤		➤				➤						PCc_A_SUM
			Offsets	Offsets	10%	10%	10%	y	➤	Y	➤		➤		➤		➤		➤						PCc_A_SUM
		Stuck in range	Stuck in range	Stuck in range	30%	30%	29%	y	➤	Y	➤		➤		➤		➤		➤						PCc_A_SUM
				Oscillation	5%	5%	5%	y	➤	Y	➤		➤		➤		➤		➤						PCc_A_SUM
Power supply	D.9	Under and Over Voltage	Under and Over Voltage	Under and Over Voltage	10%	10%	10%	y													➤		➤	Y	PCc_PSU_Mon
			Drift	Drift & Oscillation	20%	20%	20%	y													➤		➤	Y	PCc_PSU_Mon
				Power Spikes	5%	5%	5%	y													➤		➤	Y	PCc_PSU_Mon
									64.35%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		34.65%		