Automotive Mechatronic Safety Argument Framework

Roger S Rivett

Doctor of Engineering

University of York

Computer Science

June 2018

For Reg & Kath - they would have been so proud.

Abstract

A modern vehicle uses mechanical components under software control, referred to as *mechatronic systems*, to deliver its features. The software for these, and its supporting hardware, are typically developed according to the functional safety standard ISO 26262:2011. This standard requires that a safety argument is created that demonstrates that the safety requirements for an item are complete and satisfied by evidence. However, this argument only addresses the software and electronic hardware aspects of the *mechatronic system*, although safety requirements derived for these can also be allocated to the mechanical part of the *mechatronic system*. The safety requirements allocated to hardware and software also have a value of integrity assigned to them based on an assessment of the unmitigated risk. The concept of risk and integrity is expressed differently in the development of the mechanical components.

In this thesis, we address the challenge of extending the safety argument required by ISO 26262 to include the mechanical components being controlled, so creating a safety argument pattern that encompasses the complete *mechatronic system*. The approach is based on a generic model for engineering which can be applied to the development of the hardware, software and mechanical components. From this, a safety argument pattern has been derived which consequently can be applied to all three engineering disciplines of the *mechatronic system*. The harmonisation of the concept of integrity is addressed through the use of *special characteristics*. The result is a model-based assurance approach which allows an argument to be constructed for the mitigation of risk associated with a *mechatronic system* that encompasses the three engineering disciplines of the system. This approach is evaluated through interview-based case studies and the retrospective application of the approach to an existing four corner air suspension system.

Contents

List of Figures

List of Tables

Acknowledgements

I would to thank my supervisors, Tim Kelly and Ibrahim Habli, without whom I would never have embarked on this task.

I would like to thank my team at work for their forbearance and standing in for me during the times when my attention was focused on this work. I am also grateful to the staff at Jaguar Land Rover who participated in the case studies. I am in particular debt to my manager Ged Lancaster for his support and allowing me to spend so much company time on this endeavour.

Lastly, I would like to thank my wife, Rosemary, for moral support, proof reading and living without me for more time than I anticipated.

Author's Declaration

Some of the material presented in this thesis has been published in the following paper:

— Roger Rivett, Ibrahim Habli, Tim Kelly, *Automotive Functional Safety and Robustness*, International Workshops on Critical Automotive Applications: Robustness & Safety, Paris France, September 2015

This work has not previously been presented for an award at this, or any other, University. All sources are acknowledged as References.

Chapter 1 Introduction

1.1 Modern Vehicles

A modern premium passenger vehicle is a very complex machine employing many different technologies. It is potentially used all over the world in different environments by drivers who have only minimum training, [1]. In this section we give an overview of current technology and discuss the future trends.

1.1.1 Current Technology Overview

A vehicle may have up to 100 electronic control units used in its design. Each control unit will consist of hardware components (microprocessor, other VLSI components, hundreds of resistors and capacitors, 5–10 output drive devices) all surface-mounted on a multi-layer printed-circuit-board with through-hole plating. The microprocessor will typically be running anything from 32k bytes to many mega-bytes of executable code written in the C language or generated from executable models. Each control unit may be connected to sensors to read physical values related to the vehicle, the environment or driver input. Each control unit may be connected to actuators to control physical attributes of the vehicle or provide information to the driver. There are typically 50-100 sensors and actuators on the vehicle. Control units share information across multiple communication networks linked to each other by gateways and may be able to communicate wirelessly with devices external to the vehicle which also provide inputs to them. An increasing number of customer features no longer have their unique inputs and outputs but rather are functions that process data from the network, and put new data onto the network, making use of inputs and outputs associated with other features.

The physical attributes of the vehicle may be controlled by the direct conversion of electrical energy into mechanical force or movement, or by the conversion of electrical energy into pneumatic or hydraulic pressure, which in turn produces mechanical force or movement. So, the technologies involved include mechanical, hydraulic, pneumatic, electromagnetic, electrical, electronic, and software. Different control units may be able to affect the same physical attributes of the vehicle through different actuators.

The vehicle may be used by a wide variety of different people with different levels of skill, training, experience and temperament. The drivers of passenger vehicles are self-selecting; the prerequisites for being allowed to drive vary from country to country and range from merely driving for a short distance to having a specified number of hours' practice, in daytime, night time and on motorways, supplemented by a theoretical test and a practical test. Unlike crews of aircraft, ships and trains, which are required to have training on an on-going basis, drivers of passenger vehicles are not tested again unless they have broken the law or are advancing in years. Therefore, the skill level of the

drivers of a mass-produced vehicle cannot be known with certainty and it must be assumed that there is a broad spread of ability.

The primary controls of the vehicle, i.e. steering, accelerator and brakes, have become standard since first used on the 1916 Cadillac Type 53, but there are many more secondary controls with little commonisation. There is now a great impetus to add many more controls and also the availability of new technology that allows the use of new innovative controls, e.g. gesture recognition. There is an awareness of the need for good intuitive controls and of the adverse effects of this not being the case, and a growing concern about driver overload and distraction. There is very little regulation to constrain what vehicle manufacturers put into the market. The user-base is quite critical when choosing what to purchase and they are coming to judge Human Machine Interface by the standards of their smart phones and video games. Drivers may use the same vehicle over extended periods of time and become familiar with the controls, but some vehicles may be used once for only short journeys, e.g. the use of a hire car for a 'there and back' journey. While drivers should read the handbook for the controls before starting the journey, few people do this in practice. The dynamic performance and handling response of vehicles differ significantly from vehicle type to vehicle type; the driver should drive conservatively and become familiar with the behaviour and dynamic response before driving more spiritedly.

The vehicle is deployed into different countries around the world representing a diverse environment with variations in geography, climate, road surface quality, road layout, road types, junction construction, traffic density, types and numbers of other road users, traffic regulations and cultural approaches to driving. Each country has the right to control the sale of vehicles in their own country and are not subject to any wider constraints. Consequently, there is a wide variation in the detail of how regulations are written and what different countries require, although there is commonality in the major established markets, [2].

Although the vehicle has a recommended service schedule specified for its lifetime of typically ten years, it cannot be guaranteed that this service schedule is adhered to, especially once the warranty period has elapsed and the vehicle may be on its second or third owner.

1.1.2 Future Trends

The fact that modern premium vehicles are increasingly using software-based technology, [1] means that it is possible to introduce many new features to the vehicle, some of which are starting to redefine the nature of the vehicle, e.g. advanced driving assistance features such as lane keep assist. Vehicle manufacturers are introducing this technology because they want to both keep up with what competitors are doing and, for premium brands, be the first to market with new features that they hope will appeal to customers. Another reason for the use of more technology is the perception that this will help reduce death and injury on the roads. The industry and other interested

parties are promoting an ambitious future for the automobile. This is driven both by the opportunities that it creates for business and also by a generally held belief that the driver is the main cause of accidents, and that use of more technology may help reduce the number of accidents on the road, [3].

At the time of writing, there is an increasing number of new Advanced Driver Assistance Systems (ADAS) being fitted to vehicles, [4], [5]. Some of these provide additional information to the driver, e.g. parking aid, blind spot warning. Others provide positive assistance, e.g. adaptive cruise control, lane keep assist, or operate autonomously, e.g. collision avoidance by braking. Many believe that the final outcome of this trend will be driverless cars, [6], and there are already prototypes of driverless cars being used on the public roads in a number of countries.

Another area of rapid development is vehicle-to-vehicle communication networks (V2V) and vehicle-to-infrastructure communication (V2I) known collectively as V2X. This has the potential to provide vehicles with an awareness of other vehicles in their local vicinity in an urban setting. This is seen as necessary for autonomous vehicles and also opens up the possibility of vehicles being centrally controlled in a managed traffic zone, [7]. The vehicle is becoming more connected externally to the internet and the cloud.

1.2 Rise of Automotive Mechatronic Systems

While road vehicles have traditionally been primarily mechanical machines, recently, particularly since the 1970s, there has been increasing use of software-based electronic control, [8]. Starting with engine management systems and anti-lock braking, electronic control has progressively been added so that for premium vehicles virtually every mechanical function is software controlled. The combination of the mechanical components and their software control is referred to as a *mechatronic system*, [8]. In addition to those already mentioned, typical *mechatronic systems* fitted to a modern premium vehicle include steering, transmission, differentials, damping, suspension, roll control, rear spoiler, powered tailgate, powered seats and deployable door handles and tow-bar. Most of these *mechatronic systems* are safety-related in that some failures, under certain conditions, could lead to harm to people.

A *mechatronic system* is composed of a *mechanical system* and its software control, referred to as an *E/E system*. Both of these have their own and different approaches to design. Mechatronic engineering has grown out of mechanical engineering and consequently has based its approach more on mechanical design than *E/E system* design. There is no unified approach to design that reconciles both the mechanical/mechatronic approach and that of an *E/E system*.

1.3 Achieving and Assuring Safety

As mentioned above, the failure of a *mechatronic system* has the potential to cause harm. Some systems affect the driver's ability to control the motion of the vehicle, and failures of these systems could lead to an accident. Other *mechatronic systems*, such as the powered tailgate, have the ability to harm people under failure conditions through direct contact.

When a serious issue arises there is a search for the root cause; often there is not a single cause but an interplay between different aspects of the vehicle. The reports of those who experienced the issue may also lack clarity. Investigations into the issue that look at different technologies, which are actually closely linked, may suffer from not understanding the interactions. An example of the difficulty of establishing the root in such circumstances is the recall of Toyota vehicles that began in 2009, [9]. A broader approach to vehicle assurance has the potential to prevent unforeseen interactions and assist the investigation of any issues that do arise. This is what we explore.

1.3.1 The Mechanical Approach to Reducing the Potential for Harm

In purely mechanical systems, the functionality is constrained by geometry and the continuous nature of the physical properties of materials. The systems tend to have a small number of functions, for which the physics is well-established, and there are only a limited set of modes of operation. For these mechanical systems it has generally been the case that a system that does not fail is also a safe system, e.g. "*If one is examining the hydraulic system of an aircraft, the reliability of that system is more or less complementary to the safety. As reliability increases safety also increases*" [10]. For these mechanical systems, the quality techniques, whether based on reliability, robustness or the use of safety factors, were perceived to be sufficient to also address the safety issues.

1.3.2 The E/E System Approach to Reducing the Potential for Harm

This is in stark contrast to purely *mechanical systems*; the software-based electronic control systems typically have many modes of operation and the control algorithm is not constrained by physics and geometry. For these types of systems the role of non-stochastic systematic failures is at least as important as random failures and an approach to avoiding harm based purely on component reliability was seen to be insufficient, [11]. A new approach was developed from the 1970s onwards which was termed *functional safety* and this was formalised in standards such as *IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related Systems*, [12]. This was a generic standard and different industrial sectors were encouraged to produce a sector-specific version of it. In 2011 a version for the automotive industry was published, *ISO 26262: Road vehicles – Functional safety*, [13]. It is now the norm for the software, and its supporting hardware, to be developed according to this standard. While in its introduction ISO 26262 states

that it seeks to address the trend of increasing mechatronic implementation its scope is restricted to the software control provided by the *E/E system* part of the *mechatronic system*.

1.3.3 The Role of the Safety Case

The application of ISO 26262 is intended to produce an *E/E system* whose malfunction does not represent unreasonable risk to the vehicle occupants or other road users. The standard requires the development of a *safety case* which it defines as an "*argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development*". The purpose of the *safety case* is to provide an argument for the absence of unreasonable risk due to hazards caused by malfunctioning behaviour of *E/E systems*.

But, as noted above, the *E/E system* is only one part of the *mechatronic system* and so there is not a justification that the whole *mechatronic system* avoids unreasonable risk.

The standard permits functional safety requirements to be assigned to the mechanical aspects of the *mechatronic system*, which it refers to as *other technologies*, however these are considered to be outside the scope of the standard. Therefore, the safety argument only has to state that such requirements have been allocated; it does not have to justify that they have been achieved.

This is in contrast to the *E/E system* where the safety argument has to show the following:

- Safety requirements have been progressively derived, and are traceable, from the concept level down to the hardware and software
- Each safety requirement has been assigned the correct integrity value in the form of an Automotive Safety Integrity Level (ASIL) based on an assessment of the unmitigated risk
- Safety requirements at all levels have been verified as being met in the physical components
- The development of the system, hardware and software has been in accordance with the integrity requirements of the requirements being processed
- Analysis of the design has been carried out to establish that the safety requirements are not undermined by systematic or random faults
- The planning and project management was sufficient to ensure that the above were correctly carried out according to the standard

This provides the potential to have a strong safety argument for the E/E aspect of the *mechatronic system* but not the whole *mechatronic system*. We see this as a weakness, especially in a context where more and more *mechatronic systems*, of increasing complexity, are responsible for the safe control of the vehicle, either by a human driver or under direct software control. This is not to say that the development of mechanical components is in any way lacking but having a complete safety case has the potential to increase the safety assurance for the whole vehicle.

The potential benefit is not just having a complete argument; the creation of the argument requires the exchange of information and the acknowledgment of the different aspects so contributing to making a better and safer product. It is already the case that mechanical issues are sometimes managed by software, for example a software diagnostic routine may detect mechanical wear before the component fails and then take actions to mitigate the risk associated with the failure. Also, deriving safety requirements top-down has the potential to miss interactions between elements, particularly between mechanical components and *E/E systems*. Again, a complete argument has the potential to help focus attention on these interactions.

It should be noted that it is current practice to develop a *mechanical system* under *E/E system* control as a *mechatronic system*, but this is achieved informally rather than with defined mechatronic documents.

1.4 Thesis Hypothesis

Given the above, the question arises as to whether it is feasible to have a uniform approach to justifying that an automotive system, consisting of a mechanical machine controlled by software (i.e. a *mechatronic system*), is fit to be put into production from a "functional safety" perspective. This leads to the hypothesis proposed in this thesis that:

A risk-based safety argument for a complete mechatronic system can be constructed that enables the explicit and systematic derivation of safety requirements, with assigned integrity values, and that utilises evidence already produced by the established development practices for E/E systems and mechanical components.

The following explains the key terms used in the thesis hypothesis:

- **Risk-based safety argument**: one that justifies that risk has been reduced to an acceptable level
- **Mechatronic system**: a mechanical assembly under software control that relates the values measured by sensors to the behaviour of actuators, affecting the mechanical assembly, according to some stated requirements
- **Explicit and systematic derivation of safety requirements**: requirements that are traceable from the risk assessment to the lowest levels of design and which are derived as part of the co-evolution of the different technologies
- **Integrity value**: an indication of the stringency with which risk reduction measures are to be carried out

To investigate this hypothesis four thesis objectives were defined:

- TO1: To establish a design representation upon which a safety argument can be based
- TO2: To establish a safety argument pattern based on the design representation
- TO3: To establish a linkage of functional safety integrity to mechanical development
- TO4: To establish a means of providing evidence to support claims related to mechanical development

Thesis objective 1 is necessary to provide a foundation for the argument such that it can cope with the multiple levels of design and the co-evolution of the different technologies. The current work on automotive *safety cases* is based around a generic product requirements decomposition through levels of design abstraction. For an *E/E system* these are *Safety Goals*, *Functional Safety Concept*, *Technical Safety Concept*, *Hardware Safety Requirements* and *Software Safety Requirements*. We require an equivalent for the *mechatronic system* if we are to follow the same approach, which we intend to do, so as to build on existing knowledge and best practice. An argument based on levels of design abstraction will necessarily include all requirements, both nominal functionality and safety. The safety argument will be a partial instantiation of the design argument covering only safety requirements. The existing literature is reviewed to establish if a suitable description for a *mechatronic system* already exists. From the result of the literature review we document a product requirements decomposition scheme based on a generic view of design through levels of design abstraction.

Thesis objective 2 will allow an argument to be constructed for a system documented as a product requirements decomposition through levels of design abstraction for a *mechatronic system*.

Thesis objective 3 is necessary as the concept of integrity, as an indication of the stringency with which risk reduction measures are to be carried out, is not currently part of the mechanical engineering discipline.

Thesis objective 4 is necessary as it is not currently part of the mechanical engineering discipline. It provides evidence to support claims for a risk-based safety argument.

The generic mechatronic safety argument pattern is first evaluated by applying it to a generic *E/E system* definition; this allows evaluation against the current generic *E/E system* documentation. The generic mechatronic safety argument pattern is then evaluated by applying it to a generic *mechatronic system* definition; this extends the evaluation beyond the scope of existing documentation. Finally, the generic mechatronic safety argument pattern is evaluated by applying it to an existing *mechatronic system*, using extant design documentation.

1.5 Scope of work

The subject of thesis is restricted to automotive *mechatronic systems* as defined above. It only considers those aspects of mechanical development that are necessary for the safety argument and it does not address the creation of a complete safety case.

We are seeking to address a large problem space with no off-the-shelf solutions and a dearth of material directly related to our hypothesis on which we can build. We have to bridge two diverse worlds and, as such, the solution has to be generic and will have to gain the approval of both sides by being technically sound and not too onerous.

While this thesis addresses the technical aspects of product development necessary for a safety argument, it does not address the project management and planning for developing a complete *mechatronic system*; nor does it consider the governance of engineering activities, although these aspects are very important in the delivery of a safe system. The thesis only considers product development and does not include the operational, maintenance and decommissioning phases of the product lifecycle.

1.6 Contributions

1. A *model-based approach* to representing the different divisions of work necessary to create a multi-technology system, that honours the co-evolution of safety requirements, and which provides the basis for a complete risk-based safety argument for a *mechatronic system*
2. A case study on the practical application of DFMEA in an automotive OEM which assesses the extent to which, as practised, it does, or could, produce the evidence necessary to support the *mechatronic system* safety argument
3. The creation of a *mechatronic system* safety argument pattern, and its evaluation, by the application of the *model-based approach*

By taking a *model-based approach*, the argument pattern is not arbitrary but is based on an underlying understanding of the engineering task. Having a model that can represent the actual division of work between technologies and organisations facilitates its practical application.

1.7 Thesis Structure

This thesis is organised as follows:

- **Chapter 2** reviews related literature on a wide range of systems development including systems engineering, mechanical engineering, electronic/software engineering and mechatronic engineering. It reviews the societal understanding of risk and the safety standards and regulations of a number of industrial sectors. It looks at current quality and

safety practices in the automotive industry. It looks at the background and current practice regarding safety arguments.

- **Chapter 3** presents a new approach for dividing the development of a system into chunks, referred to as *Partes*, with each *Pars* being defined by a generic ontology and having a generic safety argument pattern, based on the ontology. The application of this approach to a classic *E/E system* developed according to ISO 26262 is presented.
- **Chapter 4** presents the application of the approach from chapter 3 to a *mechatronic system*.
- **Chapter 5** presents a case study of the industrial practice of DFMEA.
- **Chapter 6** presents a means by which an integrity value can be fed into the mechanical design process by the use of *special characteristics*. This is achieved by distinguishing between the means used to indicate the unmitigated risk and those used to indicate the integrity values associated with safety requirements.
- **Chapter 7** presents the evaluation of the ideas and a second case study on the *Pars* approach to partitioning the development of a *mechatronic system*.
- **Chapter 8** presents a summary of the main conclusions of this research and identifies several areas for further work.
- **Appendix A** presents a fuller exposition of the DFMEA.
- **Appendix B** presents a fuller exposition of ISO 26262.
- **Appendix C** shows how the generic safety argument pattern for a *Pars* can be used to express the safety argument for an existing system.
- **Appendix D** presents a case study evaluating the practicality of the *Pars* approach.
- **Appendix E** lists the *Pars* approach evaluation case study questions.
- **Appendix F** lists the DFMEA usage case study questions.

Chapter 2 Literature Review

As described in Chapter 1, *mechatronic systems* may be complex and their creation may involve many different engineering disciplines. These disciplines have their own theoretical bases, established processes, practices and methods and their own approach to risk management.

This chapter presents a review of related literature covering the topics of systems engineering, risk, product assurance and safety arguments. It starts with a review of general systems engineering and in particular the role of architectures and the derivation of requirements. It then reviews the literature on *mechatronic systems*, *mechanical design* and *E/E system design*. The sociological view of risk is reviewed before looking at how risk is addressed in different industry sectors through the use of regulations and standards. It then looks at how product assurance is practiced in industry with regard to both quality and safety. Lastly, it reviews the literature on safety cases.

2.1 Systems Engineering

Modern systems engineering encompasses many different domains including management, engineering, technical, social, human and political/legal, [14]. There is the commercial business case that considers the cost of development, manufacture, operation and service and the anticipated return on investment. There are also technical aspects including the gathering of requirements, the detailed design of the parts and the creation of operating and maintenance instructions. The discipline of systems engineering does not have a specific beginning, but most authors see it as being formally developed since the 1940s when the term was first used at Bell Telephone Laboratories. The need to take this new approach was driven by the increasing complexity of the machines using new technologies and particularly computer control, [15], [14].

The International Council on Systems Engineering (INCOSE), which is a non-profit membership organization with the world's largest professional network of systems engineers, defines systems engineering as: *"an engineering discipline whose responsibility is creating and executing an interdisciplinary process to ensure that the customer and stakeholder's needs are satisfied in a high quality, trustworthy, cost efficient and schedule compliant manner throughout a system's entire life cycle. This process is usually comprised of the following seven tasks: state the problem, investigate alternatives, model the system, integrate, launch the system, assess performance, and re-evaluate.*", [16].

NASA defines systems engineering as: "*a methodical, disciplined approach for the design, realization, technical management, operations, and retirement of a system.*" and a system as: "*a construct or collection of different elements that together produce results not obtainable by the elements alone. The elements, or parts, can include people, hardware, software, facilities, policies, and documents.*", [17].

One significant aspect of the systems engineering approach is the consideration of all the stakeholders; typically, these include end users, operators, maintainers, suppliers, acquirers, owners, regulatory agencies and manufacturers. ISO 15288, [18], is a standard that provides a framework to improve communication and co-operation among such disciplines. The standard assumes that an organisation operates according to a defined system life cycle model. It does not prescribe a particular model but acknowledges that the following are typical life cycle stages: concept, development, production, utilisation, support and retirement. It defines a set of life cycle processes that can be used within any system life cycle model. The processes are presented in four groups: Agreement Processes, Organizational Project-Enabling Processes, Technical Management Processes and Technical Processes. The Technical Processes are shown in Table 1.

Business or Mission Analysis Process
Stakeholder Needs & Requirements Definition Process
System Requirements Definition Process
Architectural Definition Process
Design Definition Process
System Analysis Process
Implementation Process
Integration Process
Verification Process
Transition Process
Validation Process
Operation Process
Maintenance Process
Disposal Process

Table 1: ISO 15288 - Figure 4 System life cycle processes [18]

An example of a typical system life cycle, taken from Stevens *et al*, [19], is shown in Figure 1.

2.1.1 Architecture

A key aspect of the technical process is the architecture design. ISO 15288, in common with ISO 42010, [20], defines a system architecture as: "*fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution*". This is important because a system is a construction or collection of elements to produce results, [17], and the architecture defines the arrangement of these elements such that the desired result is obtained. According to ISO 15288, the system architecture defines the boundaries of the system and those interfaces to external entities which are necessary to support essential architectural decisions. It also defines the elements of the architecture and their relationships. The architecture is based on those stakeholder requirements which drive the architecture definition. The remaining requirements are addressed in the design of the system elements.

The ISO 42010 standard provides a core ontology for the description of architectures. It defines the key concepts related systems and their architectures as shown in Figure 2.

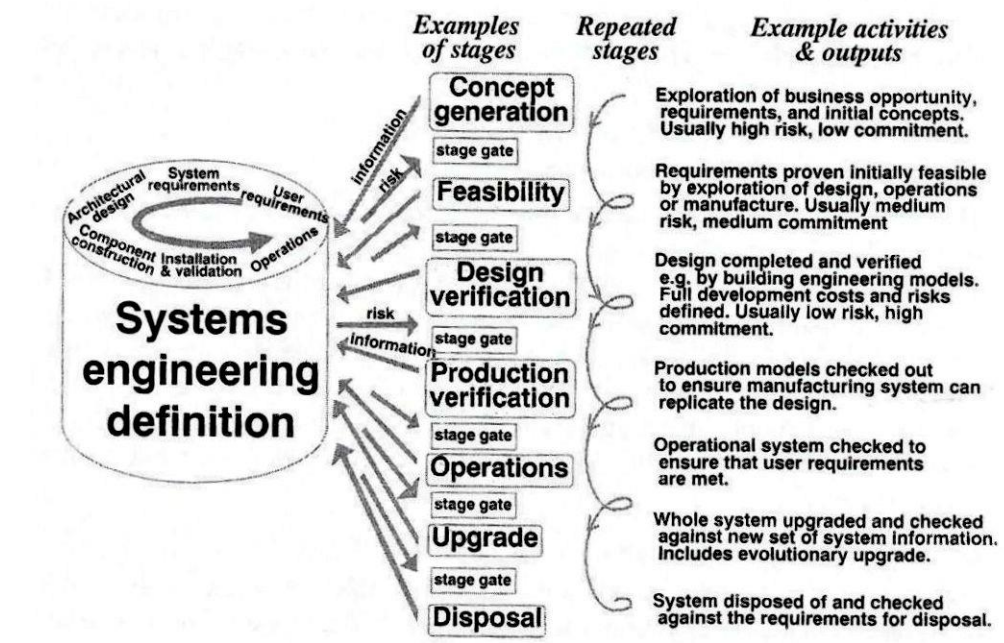

Figure 1: Example of typical system life cycle [19]

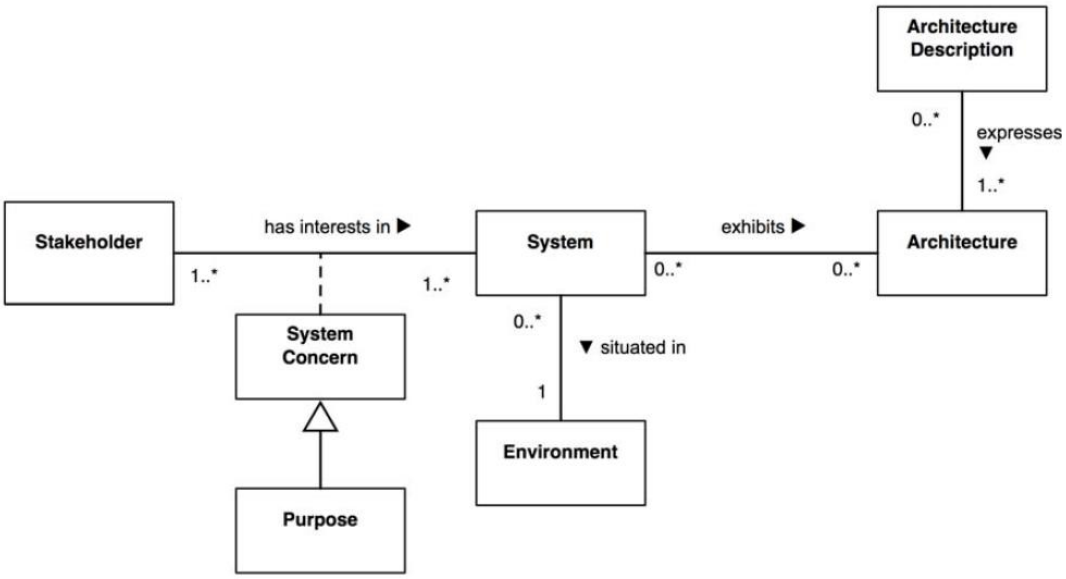

Figure 2: ISO 42010 [20] - Figure 1 Context of architecture description

It defines the conceptual model of an architecture description as shown in Figure 3

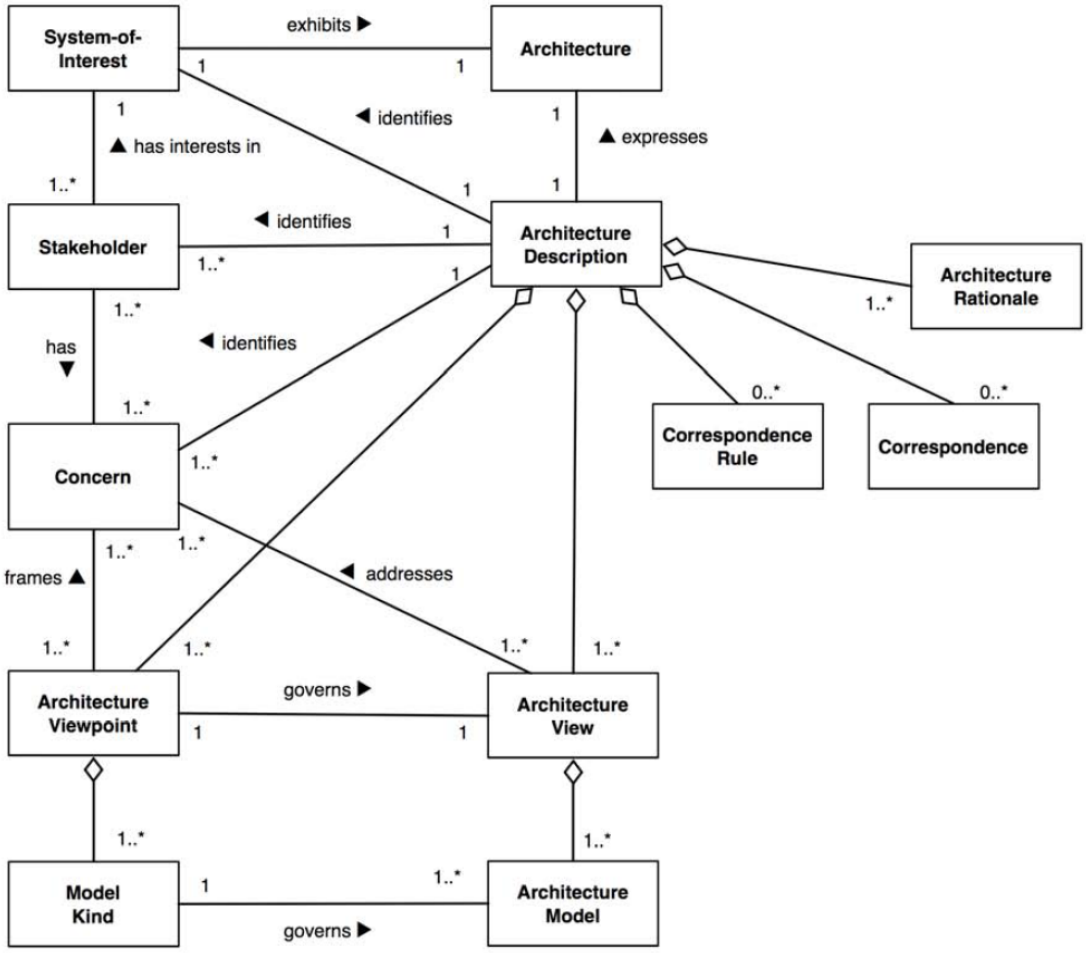

Figure 3: ISO 42010 Systems [20] - Figure 2 Conceptual model of an architecture description

Zachman, [21], has also identified the need to use an architecture framework for defining and controlling the interfaces and the integration of all of the components of the system. First defined in 1987, [22], version 3 was released in 2011. The Zackman framework is based on a 6 x 6 matrix. The six columns are entitled: what, how, where, who, when, and why. The six rows represent the enterprise at different levels of abstraction, e.g. business level to technical level. The Zachman framework is used principally for the development of enterprise systems.

Work has been carried out on defining automotive architecture frameworks, Dajsuren *et al*, [23], and Broy *et al*, [24]. Both are based on ISO 42010, [20]. Dajsuren *et al* define an Automotive Architecture Framework designed to describe the entire vehicle system across all functional and engineering domains. They define an automotive version of Figure 3 and formally define correspondence rules between functional and software views. The scope of their work is wider than a *mechatronic system*, which is not explicitly mentioned. They do not address the allocation of software to hardware compute components. Similarly, *Broy et al* define a Meta Architecture Framework to describe the whole vehicle. Again, their model is high level using abstraction levels of function, logical and technical elements and a generic system decomposition of System levels 0, 1, 2.

2.1.2 Requirements

All the literature concerning systems engineering stresses the need to understand the requirements of the different stakeholders, particularly those of the user and the customer. The ISO 15288 process requires stakeholders to be identified and their needs and priorities documented as requirements.

As most modern-day systems are controlled by software, much of the material on requirements elicitation and expression is written from the software perspective. The *use case* approach became a mainstay of software development with the publication of Jacobson's book in 1992, [25]. *Use cases* are included in the OMG UML specification, [26], and also the OMG SysML specification, [27], where they are defined as a specification of behaviour. In UML/SysML, *use cases* capture the requirements of systems by recording the interactions between the system and the actors external to the system; these include both human users and systems that may interact with a subject. The human users represent some of the stakeholders of the system. As Fowler notes, [28], *use cases* can be used to capture user goals and user interactions with the system. The *use case* approach can also be extended to document negative scenarios, referred to as *misuse cases*, [29]. The term *scenario* is also used. Fowler, [28], describes a *scenario* as a single path through a *use case* as determined by a particular combination of conditions. Other writers consider a *scenario* to be a more informal story-based description of the way that users interact with the system, focusing on particular instances rather than abstract description, [30].

Both Jackson and Parnas consider a more formal way of relating the behaviour in the environment and the requirements of the software. In his 1996 paper, Jackson, [31], draws a sharp distinction between the environment, or world, and the machine and takes the view that requirements describe the world as it will become as a result of the machine. The gap between the world as it is now and how it could be in the future is referred to as the *problem*. His *problem frame scheme* is based on defining actions that are controlled by the world, controlled by the machine or shared by the world and the machine. This provides a means of structuring the analysis of the problem in the world by capturing the characteristics and interconnections of the parts of the world it is concerned with, and the concerns and difficulties that are likely to arise in discovering its solution. *Problem frames* do not aim to capture classes of problems of realistic size and complexity but rather provide a means of splitting these into sub-problems, [32]. In his 2002 paper, [33], Jackson considers the links between the problem domain, environment, and the solution domain; for him, this is the software architecture.

Parnas, [34], is motivated by the need to have adequate software documentation. He defines a relation *NAT* to describe the environment, i.e. the world outside the system to be developed, including previously installed systems, without making any assumptions about the system. The *NAT*

relation is an ordered pair of values in the environment that can be monitored, and values that can be controlled. The relation constrains what values the quantities can take. In Jackson's terms, this represents the world as it is. The requirements for the system to be developed are described by the relation *REQ* which is another ordered pair of values in the environment that can be monitored and values that can be controlled. To be valid, the domain of *REQ* must be a subset of the domain of *NAT*. Parnas assumes that the system will comprise input devices, software running on a processor and output devices. The input devices monitor variables in the environment and present representations of their values to the software. The output devices take values produced by the software and update the controlled variables in the environment. The behaviour of the input devices is described by the relation *IN*, which is an ordered pair of the values of the monitored quantities and the processor input register values. The behaviour of the processor output devices is described by the relation *OUT*, which is an ordered pair of output register values and controlled quantities. The Software Requirements Document describes the relations *NAT*, *REQ*, *IN*, and *OUT*. The input-output behaviour of the system is described by the relation *SOF*, which is an ordered pair of input register values and output register values. If the relations *NAT*, *IN*, *OUT*, and *SOF* are valid for a defined range of values, then this implies that the *REQ* relation is also valid.

There are also *requirements-capture techniques*, under the banner of goal-oriented, used in particular for acquiring organisational and business requirements. The two major techniques are KAOS, [35] and the i* [36].

Many authors recognise that capturing the system requirements and defining a system architecture are not performed just once during the development of the system, but rather that there is a continuous back and forth between requirements and the architecture as the system development progresses and the system solution emerges. This is illustrated by Figure 4 taken from Stevens *et al*, [19].

Nuseibeh, [37], working with the *problem frame paradigm*, describes an adaptation of the *spiral lifecycle model* informally referred to as the *Twin Peaks model* to emphasize the equal status given to requirements and architectures. The model develops requirements and architectural specifications concurrently, while maintaining a separation of the problem structure and specification from the solution structure and specification. It is an iterative process that produces progressively more detailed requirements and design specifications, see Figure 5.

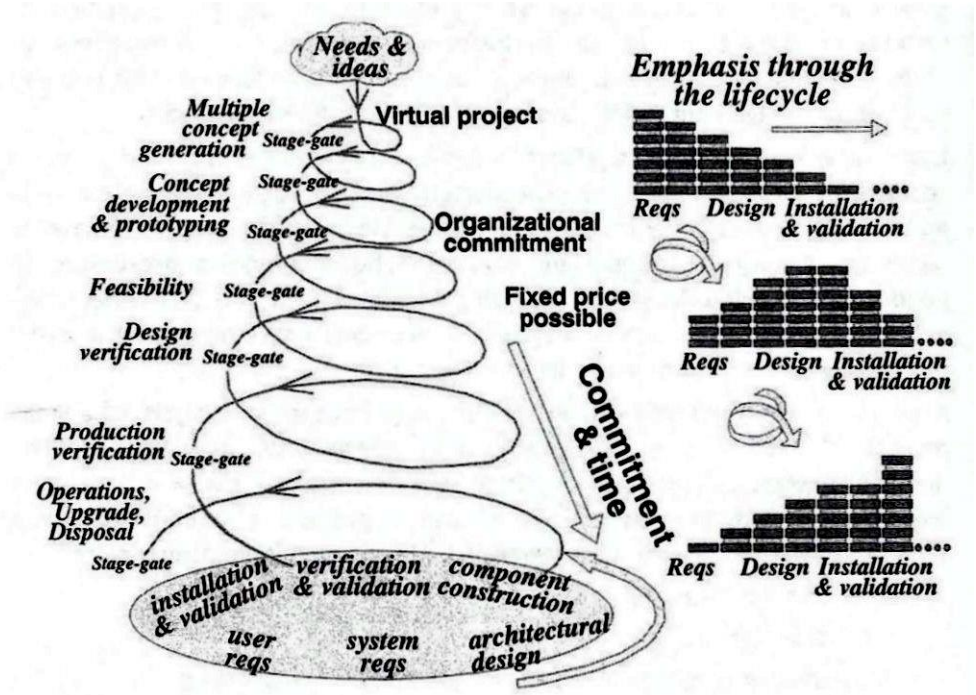

Figure 4: System evolution during the life cycle [19]

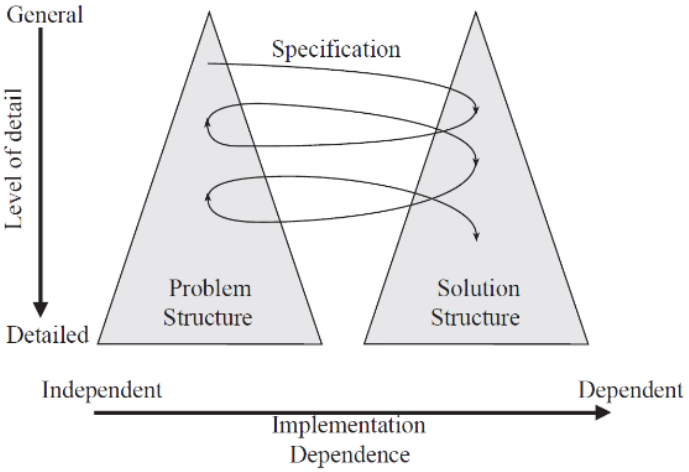

Figure 5: Twin Peaks Model taken from [33] unmodified

In [33], the *problem frame* approach is developed to allow architectural design concerns to be incorporated during problem analysis. The paper acknowledges that, when working within an established engineering area, many of the software services that will be required of the machine already exist, and it is inefficient not to recognise this in the analysis. The approach taken is to annotate the machine domain with the existing services. This way they appear in the *problem frame* while also appearing within the machine, and hence the solution domain.

2.1.3 Mechatronic Systems

At the beginning of the twentieth century mechanical devices started to include electrical components and then in the 1940s, during World War II, electronic control systems. These

electronic systems have matured from very simple functions and logic to the incorporation of computers and complex logic, [38]. Systems that have mechanical, electronic, and software components are often called *mechatronic systems*.

Since 1971, the number of systems that can be included under the umbrella term of mechatronic has been growing rapidly, driven by the availability of increasingly powerful microcontrollers, [39]. As an example, during this time the automobile has evolved from a primarily mechanical machine to one that can be viewed as a collection of *mechatronic systems*, with such systems controlling the engine, brakes, steering, locking and doors, windows and lights, [39]. The Advanced Driver Assistance Systems (ADAS) are all achieved through *mechatronic systems*, as will be the autonomous vehicle.

The term *mechatronics* was first coined by the Yasakawa Electric Company which, in their 1971 trademark application, defined it in the following terms: "*The word mechatronics is composed of 'mecha' from mechanism and the 'tronics' from electronics. In other words, technologies and developed products will be incorporating electronics more and more intimately and organically into mechanisms, making it impossible to tell where one ends and the other begins".* Since then, other variations of this definition have been proposed, but all capture the sense of electronic control of mechanical systems, where electronic control is understood to include software control, [39].
While a *mechatronic system* consists of a mechanical machine under electronic control, the engineering discipline of *mechatronics* embraces all the subject matter necessary to specify and develop such systems. This includes the modelling and simulation of the mechanical machine, the sensors and the actuators, and also the development of the control system. For example, the French standard NF E 01-010 defines *mechatronics* as an "*approach aiming at the synergistic integration of mechanics, electronics, control theory, and computer science within product design and manufacturing, in order to improve and/or optimize its functionality*", [40]. While Isermann, in [39], defines *mechatronics* as an interdisciplinary field, in which the following disciplines act together:

- mechanical systems (mechanical elements, machines, precision mechanics)
- electronic systems (microelectronics, power electronics, sensor and actuator technology)
- information technology (systems theory, automation, software engineering, artificial intelligence)

Bradley, [41], suggests that *mechatronics* now has to be seen as encompassing a holistic view of system design and development and not just the integration of electronics with mechanical engineering and software.

Mechatronic systems presuppose a basic system design as shown in Figure 6, [42], [43].

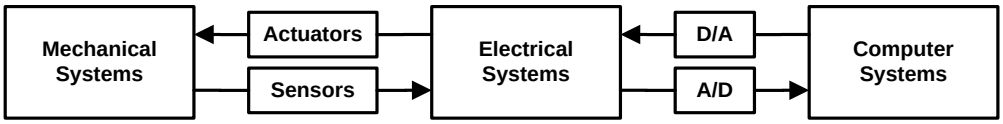

Figure 6: Generic Mechatronic System Design taken from [42] unmodified

A *mechatronics* design process suggested by Shetty and Kolk, [42], is shown in Figure 7. This clearly shows the prominent role played by modelling and simulation in the development of a *mechatronic system*. What is noticeable is that design of the electronic hardware and the software that drives the hardware and the sensors and actuators is not mentioned. Nor is the translation of the control model into the embedded software to be run on the target hardware mentioned.

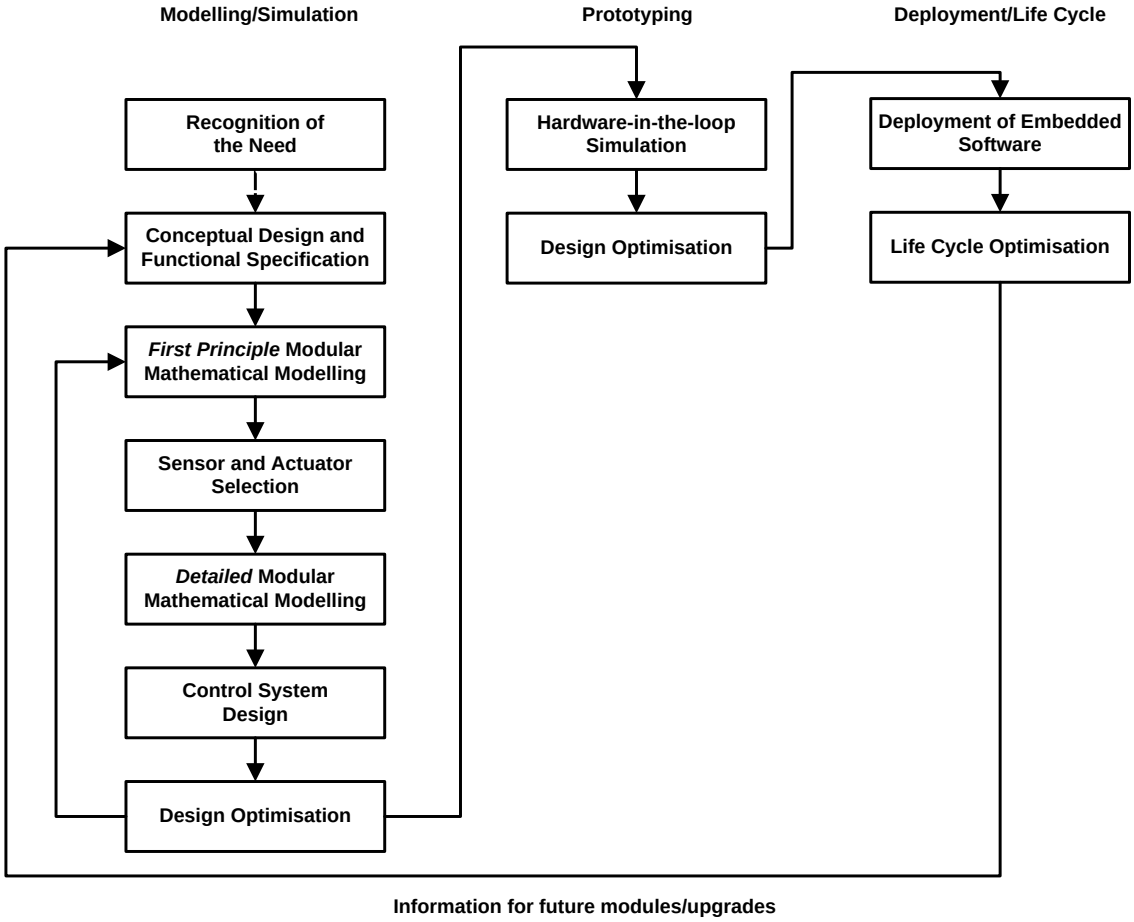

Figure 7: Mechatronic Design Process taken from [42] unmodified

Given the presupposed system design, much of the established literature on mechatronic systems, [42], [39], [44], majors on three key topics: understanding the control requirements of the plant or process by modelling both the plant/process to be controlled and also the actuators that enable the control to be enacted; understanding how parameters of the plant can be measured by sensors and the data transferred to the control processor; the design of a software control system to meet the control requirements of the plant/process given the limitations of the sensors, actuators and control processing unit. These activities are largely confined to the ISO 15288 technical processes for

Stakeholder Needs & Requirements Definition, System Requirements Definition, Architectural Definition, Design Definition and System Analysis.

Noting that, unlike traditional design processes, a mechatronic design process integrates multiple engineering disciplines, Follmer *et al*, [45], seek to address a perceived lack of a mechatronic concept design process by the use of SysML for creating system-level models. Their goal is to represent the overall system in a way that gives equal weight to all engineering disciplines involved, especially the *non-material* components (e.g. software components). The mechatronic systems are systems-of-systems and the system-level models illustrate the dependencies between the sub-systems which themselves may consist of solutions from different engineering disciplines.

Johar and Stetter, [46], also seek to provide a description of the mechatronic life cycle which gives equal weight to the different engineering disciplines involved. They base a version of the systems V life cycle on VDI 2206, [47] and the design methodology of Pahl and Beitz [48]. In their example, they use UML *use case* diagrams to model the overall system from which a requirement list is created. The requirement list is further refined using more *use case* diagrams to give more details. The concept design is supported by a class diagram. The design embodiment now follows and the systems V life cycle, Figure 8, shows how the system is divided into three engineering domains. A UML class diagram is created for each engineering domain as a reference for the creation of the respective requirement analysis.

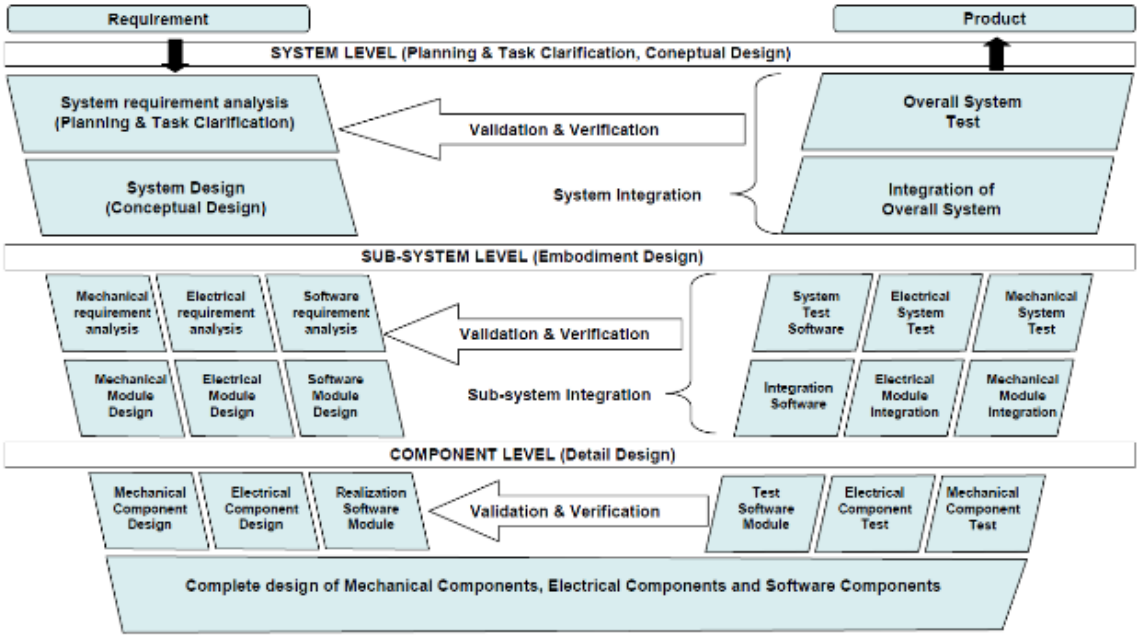

Figure 1. Combined structure of a design process for mechatronical products

Figure 8: Mechatronic system V life cycle taken from [46] unmodified

Sell and Tamre, [49] also seek to use SysML to provide a common language which can unite the different engineering disciplines involved in creating a mechatronic system They also base their

approach on the V-model from VDI 2206, [47]. Mhenni *et al*, [50], also use SysML in their proposed mechatronic system design methodology. It consists of two phases: a black box analysis with an external point of view that provides a comprehensive and consistent set of requirements, and a white box analysis that progressively leads to the internal architecture and behaviour of the system.

2.1.4 Mechanical Design

Efforts to produce a systematic design process date from at least the 1920, [51]. At this time the emphasis was on mechanical engineering. An influential mechanical design method is *Systematic Approach,* described by Pahl and Beitz in their book *Konstruktionslehre,* published in German in 1977 and translated into English in 1988 as *Engineering Design - A Systematic Approach*. The third edition was published in English in 2007 [48]. Their overall approach is shown in Figure 9.

The requirements list is based on the market analysis and consumer-specific technical performance requirements and includes geometry, kinematics, forces, energy, material, signals, safety ergonomics, production, quality control, assembly, transport, operation, maintenance, recycling, costs and schedules. The concept of an architecture is not used, however in a chapter on mechatronic systems the authors borrow the generic mechatronic system design from Isermann, [43]. Verification is not a separate step in the process but rather an intrinsic part of embodiment design. There is no concept of validation. An ontology of the concepts behind their systematic approach is shown in Figure 10.

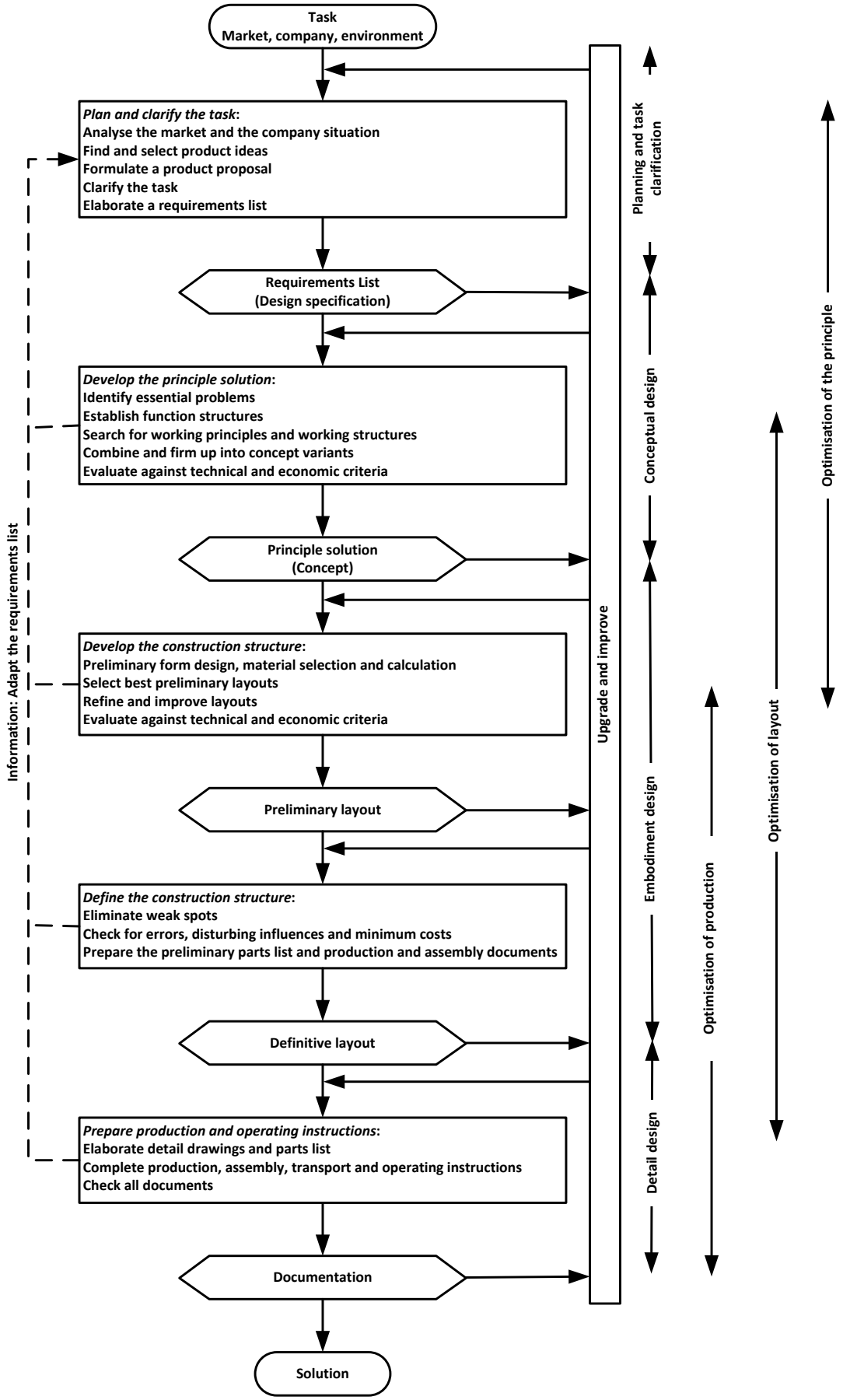

Figure 9: Steps in the planning and design process taken from [48]

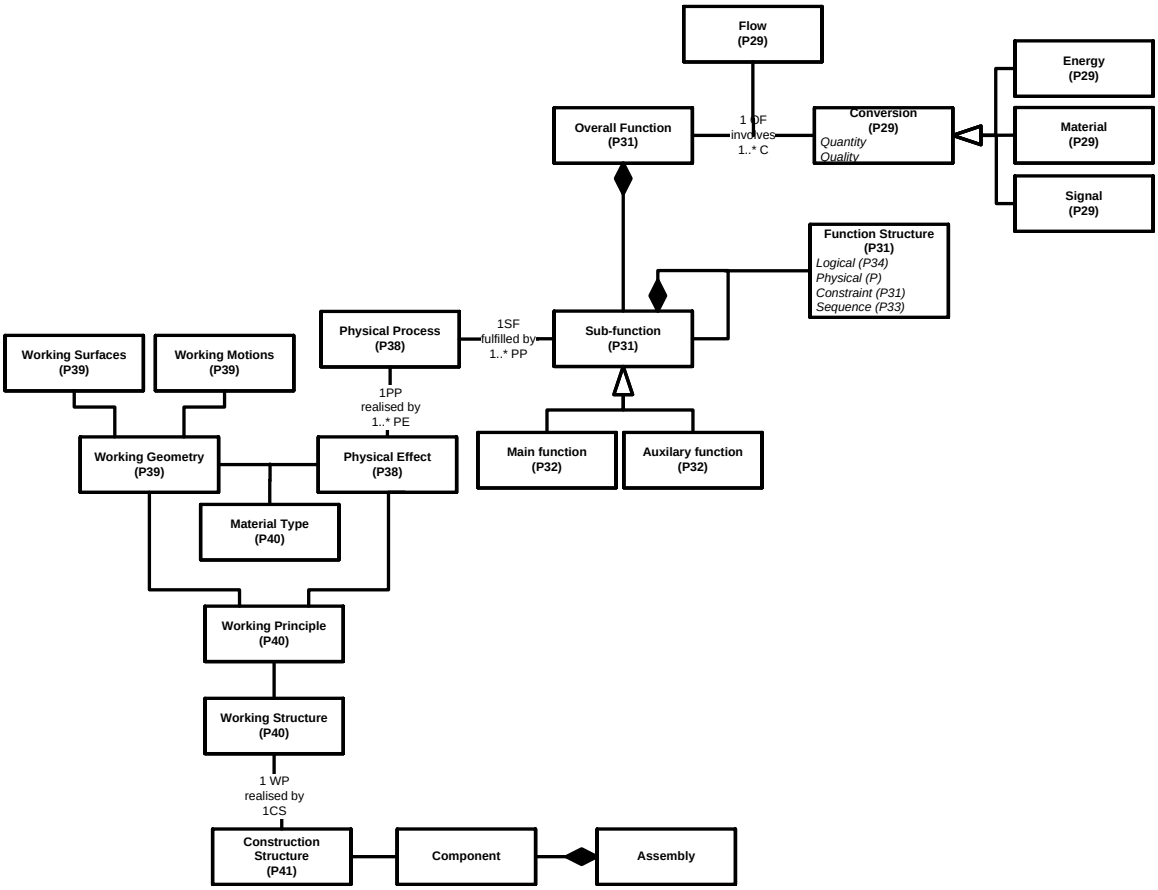

Figure 10: Ontology of Pahl & Beitz Systematic Design

In systematic design, the overall function is seen as a flow by which energy, material and/or signals (information) undergo a conversion. The sub-functions that realise the overall function are fulfilled by a physical process realised by physical effect. The physical effect is achieved by a working principle exploiting the geometry and material properties of a physical structure.

The design process proposed by Ullman, [38], is shown in Figure 11. Ullman emphasises the need to understand the customer requirements and describes the Quality Function Deployment method as a means of achieving this. For Ullman, the architecture is the form of the product, i.e. its shape, its colour, its texture and other factors relating to its structure. Verification is not mentioned and there is a single mention of concept validation by consumers under project planning.

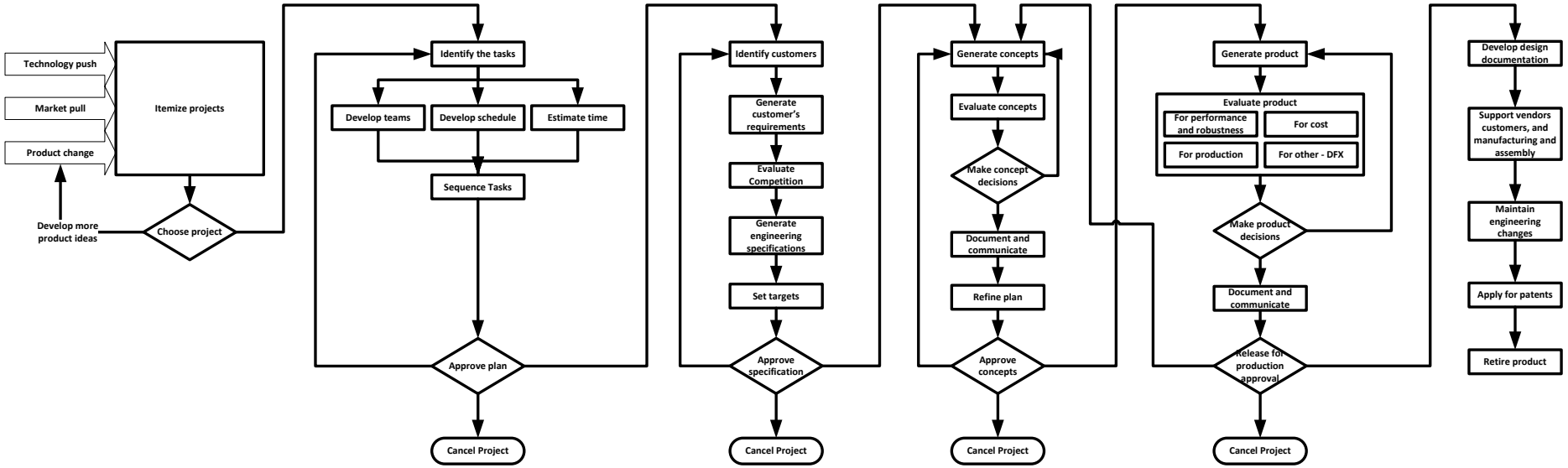

Figure 11: Mechanical design process taken from [38]

An ontology of the concepts used by Ullman is shown in Figure 12.

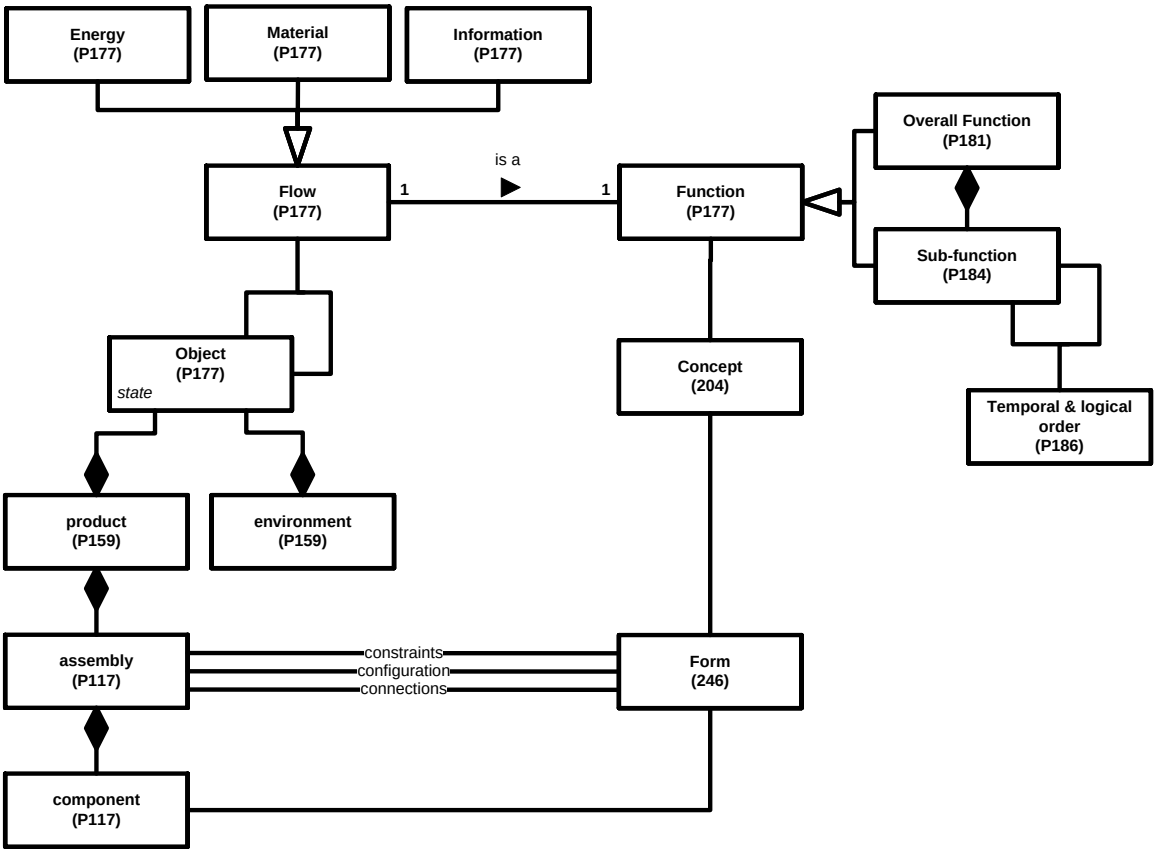

Figure 12: Ontology of Ullman concepts

Again, we see that a function is defined as a flow of energy, material and/or information and the flow is achieved via a physical form realised as components and assemblies. Kossiakoff *et al*, [14], also view systems as essentially operating on three basic media: information, material and energy.

2.1.5 E/E System Design

E/E system (electrical and/or electronic system) is a term used within the automotive industry to refer to electronic control units. It is defined in the automotive functional safety standard ISO 26262, [13], as a "*system that consists of electrical and/or electronic elements, including programmable electronic elements*". System is defined as a "*set of elements that relates at least a sensor, a controller and an actuator with one another*" and an element is defined as a "*system or part of a system including components, hardware, software, hardware parts, and software units*".

There is little literature specifically on the development of *E/E systems* as such, while there is a large corpus of material of software development and hardware development. Some mention of software development is made in system engineering literature where the classic software V life cycle is presented with process steps of software requirements, architecture design and detailed design, together with their corresponding verification steps, [19], [14]. The development of

electronic hardware is not included in this material. The best treatment is actually in the functional safety standards, and here we use ISO 26262, [13], as a reference.

Hardware

Requirements for electronic hardware typically concern the relationship between digital and analogue inputs and digital and analogue outputs, the performance (e.g. speed resolution, capacity) and the environmental conditions it has to work in (e.g. EMC, temperature, humidity).

ISO 26262 describes a hardware life cycle that starts with the specification of hardware safety requirements based on the system design and the hardware-software interface definition. This is followed by the production of a hardware design architecture and then the detailed design. The detailed design is verified, then all the hardware is integrated and the whole design is verified. Hardware-software integration and testing is considered to be part of system design.

Software

Kossiakoff *et al*, [14], referring to software intensive systems where the majority of the functionality is in software, state that the life cycle model for the software development is very similar to that of the systems development. ISO 26262 describes a software life cycle that starts with the specification of software safety requirements based on the system design and the hardware-software interface definition. This is followed by the production of a software design architecture and then the software unit design and implementation. Software unit verification is followed by software integration and verification. Hardware-software integration and testing is considered to be part of system design.

As the software requirements are cascaded from the system design the literature on requirements reviewed above is only relevant at the system level.

2.1.6 Systems Engineering Discussion

Clearly, mechatronic engineering fits in well with the system engineering approach as both systems engineering and mechanical literature make references to *mechatronic systems*.

The *requirement literature* reviewed concentrated on requirements coming from people or systems in the environment. An emphasis on software requirements tends focus on problems and solutions in the discrete domain, whereas mechatronic problems have a large continuous domain aspect to them. The requirements for controlling a real-time mechanical system also come from the nature of the actuator interfacing with the mechanical system and the mechanical system interacting with its external environment. Hence the prominence of modelling in mechatronic engineering to determine these types of requirements.

Both Jackson, [33] and Parnas, [34], only address software requirements; *mechatronic systems* use many different technologies including hardware and software. Therefore, it is more appropriate to

focus on system requirements. While some principles of Jackson and Parnas may be valid at the system level, the detail of the exposition does fit well at the system level. In the system design paradigm, software requirements, like other technological requirements are principally derived from the system design and supplemented by requirements specific to the technology chosen to implement the design.

Defining a system and then capturing requirements for it always involves deciding where the boundary lies between the system and the external world, or environment. Different authors draw the boundary in different places. This topic was discussed by MISRA in [52], which identified three different boundaries: the boundary of the target of evaluation, the zone of responsibility and the system boundary. Where the boundary is placed can be influenced by a number of factors including technology, scope of responsibility or interaction with other systems. With the tendency for systems to be connected together to form largescale complex IT systems, it becomes increasingly difficult to decide where the boundary should be. Where the boundary is drawn determines who the stakeholders are. ISO 15288, [18], notes that a stakeholder's perception of a system boundary depends on their interests and responsibilities, and gives guidance that the boundaries should encapsulate meaningful needs and practical solutions. Kossiakoff *et al*, [14], also stress the need to precisely define the boundary. They suggest that the following be taken into account in defining the boundary: development control, operational control functional allocation and unity of purpose. Differences seen in the literature in the construction of *use cases* and *scenarios* are caused by the different boundaries chosen.

It is noted that, although the concept of an architecture features heavily in *Systems Engineering* and in *E/E systems* as a description of the design, it is not used this way in mechanical engineering where, if used at all, it refers to the physical form of the solution.

The concept of the design evolving through levels of abstraction as requirements and architectures and refined through an iterative process that produces progressively more detailed requirements and design specifications, [37], can be applied to a *mechatronic system*. Mechanical design does not have the sense of cascading and refining requirements; rather, it is the design concepts and implementation that are refined. It is perhaps for this reason that the concepts of verification and validation do not feature heavily in mechanical design processes and these are considered to be an integral part of the design embodiment.

The work on automotive architectures, [23], [24], while instructive, does not provide the basis we are looking for so that an argument can be applied at the highest level of abstraction down to the lowest.

The overall summary is that systems engineering emphasises the cradle-to-grave nature of development, while mechatronics emphasises the modelling of the plant, the sensors and actuators

and the software control. The mechanical literature emphases the derivation of form to provide function, while embedded control emphases joint development of hardware and software. There is no standard hardware development process and the concept an *E/E system* development has arisen from the functional safety standards. The challenge of a unifying principle from which a common safety argument can be derived remains.

2.2 Risk

Risk is a human construct, not a property of the world; before consciousness there is no concept of risk. As Hansson says, "*risks do not simply 'exist': they are taken, run, or imposed*", [53]. In the 1960s and 1970s attempts were made to determine a level of 'acceptable risk', but it soon became clear that this cannot be done, since the acceptability of a risk-generating activity depends not only on the risk but also on the associated benefits, Bicevskis, [54] and Rowe, [55]. As we will see, risk is partly a cultural construction as well as an individual construction in that different societies worry about different risks at different times. We are interested in the nature of the relationship between risk, as perceived and managed at the societal level, and the engineering approaches to failure, uncertainty and risk associated with our man-made mechatronic systems.

We take a top-down approach and first look at general public perceptions of risk as documented by sociologists and other commentators. As it is the public who are ultimately exposed to the risk posed by the product, we are interested to see if there is a firm basis for the definition of risk that is accepted by the public. If such a thing exists it can be thought of a top-level customer requirement. We then look at how societal agencies seek to manage risk and what they base their criteria on. We are interested in this because the outcome of societal agencies is legislation and standards which engineering work has to comply with. Lastly, we look at the engineering practice and the theory underlying this.

2.2.1 Sociological View of risk

The Risk Society

There have been many books published recently commenting on the public perception of risk. Gardner, [56], comments that: "*We are the healthiest, wealthiest, and longest-lived people in history. And we are increasingly afraid. This is one of the great paradoxes of our time*". He suggests that the reason that modern societies are so unnecessarily frightened is due to a number of factors. For example, we do not know our history; things were much worse for our ancestors but we become habituated to the present circumstances. It is in the interest of many people for us to be so, e.g. people with something to sell to protect us, politicians who want to create a role for themselves as our protectors, people who desire funding and/or a public profile and the media who need attention-

grabbing stories. Also, our cultural upbringing sensitises us to some risks and desensitises us to others; in this he quotes the work of Daniel Kahneman.

Kahneman, a psychologist, in his 2012 book *Thinking, Fast and Slow*, [57], describes two approaches that the human brain uses for making decisions which he refers to as System 1 which "*operates automatically and quickly, with little or no effort and no sense of voluntary control*" and System 2 which "*allocates attention to the effortful mental activities that demand it, including complex computation*". He also accepts that we are unnecessarily afraid and explains this as the effect of System 1 thinking which is adversely influenced by the points that Gardiner highlighted. While experts formulate risk in objective probabilistic terms, [58], Kahneman notes that this is not how the general public perceive risk and quotes Paul Slovic, [59]: "*'Risk' does not exist 'out there', independent of our minds and cultures, waiting to be measured. Human beings have invented the concept of 'risk' to help them understand and cope with the dangers and uncertainties of life. Although these dangers are real, there is no such thing as 'real risk' or 'objective risk'*". These different approaches to risk are also recognised by Blastland and Spiegelhalter in their populist book *The NORM Chronicles*, [60], where they describe two faces of risk: "*one impassive, formal, calculating, the other full of human hopes and fears*". They conclude that these two faces of risk are incompatible; for people, there is no such thing as probability.

We see from the above that there is no absolute concept of risk as perceived by the general public, but rather the perception is contextual, not necessarily consistent with regard to different sources and subject to change over time.

Sociologists have written much about the relationship between the modern world and the perception of risk, and the term *risk society* was coined in the 1980s to capture the change that was perceived to have occurred during the last century. The sociologist Ulrich Beck, in his book *Risk Society: Towards a New Modernity*, [61], defines the *risk society* as: "*a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself*".

Gardner, [56], comments that sociologists broadly agree that people living today in modern countries worry more than those who lived in previous generations, with some saying that we live in a culture of fear. He notes that Beck, [18], was one of the first to understand that modern countries were becoming nations of worriers. Beck coined the term *risk society* to articulate this heightened concern about risk, particularly that caused by modern technology. Beck, [61], himself commented that: "*We are more afraid than ever because we are at more risk than ever. Technology is outstripping our ability to control it*". Gardner, [56], challenges Beck's view that we are more at risk than ever by quoting several figures including life expectancy and quality of life.

The foundation of Beck's sociological work has been challenged by other sociologists, for example Elliott, [62], who argues that Beck's work contains several sociological weaknesses: "*a dependence*

upon objectivistic and instrumental models of the social construction of risk and uncertainty in social relations, and a failure to adequately define the relations between institutional dynamism on the one hand and self-referentiality and critical reflection on the other". Other criticisms of Beck's work by sociologists are mentioned in Zinn's review of risk and sociology, [63].

Adams, [64], acknowledges that at a time when people in the wealthier nations are enjoying greater wealth, health and longevity, they are increasingly anxious about risk and find it difficult to trust government, industry and science; at the same time people are increasingly allowing those professionals who specialise in risk to control their lives.

Although this latter point is challenged by Otway and Von Winterfeldt, [65], Adams sees a number of different ways in which individuals can respond to this. One way, called *egalitarian,* is to move to a small-scale sustainability model; another way, called *hierarchist*, is to trust in more effective management; the last way, called *individualist*, and expected to be the most common, is to concentrate on the benefits and trust market forces to contain them. This last response is also known as *resigned fatalism*.

Commenting on Beck, Jarvis, [66], notes that the real issue is about how we perceive, manage, compensate and mitigate risk, rather than any increase in the number of risks. He thinks that Beck has identified "*a global society ill at ease*" and exposed a number of paradoxes. On the one hand, people are aware of the success of science and technology and their inroads into every aspect of everyday life, and the benefits to collective welfare that result. At the same time, people still face the dangers of everyday life, including the negative impact of exposure to the outcomes (products) of scientific progress. Aven, [26], has also looked at criticisms of Beck's work and has come to the conclusion that his views on risk and risk analysis should not be dismissed.

An earlier sociological study of risk was made by Douglas & Wildavsky, [67], who thought that what people choose to fear depended on the culture they were in and the groups that they interacted with socially; their principal example was the rise of the environmental movement. This has in turn been criticised. Elliott, [62], in a review of Douglas and Wildavsky, admits that they: "*make a provocative and … original point when they call attention to risk selection as a social process.*" However, he maintains that this is not an entirely successful explanation of risk.

State Response

The *risk society* approach to understanding modern attitudes towards risk has been criticised by Hood, Rothstein and Baldwin in *The Government of Risk*, [68]. They understand Beck to believe that the significance of risk to everyday life differs between historical periods. Examples of risks of concern to the current period include genetically modified organisms, reproductive technology and computer failures which potentially have wide-scale impact. Whatever the accuracy of the idea that

the current period of time is a *risk society* in contrast to earlier periods, they claim it cannot be denied that there is currently a considerable amount of discussion and literature on risk, hazard and blame and that this needs an explanation. They are of the view that: "*society-wide generalisations about risk regulation have little power to explain why risk regulation regimes differ from one another. The same point seems to apply to the analysis of regulatory dynamics. … to predict or explain them in detail we need to pay close attention to differences in historical context and the way institutional filters work*".

Hood, Rothstein and Baldwin, [68], also note that we live in a regulatory state, by which is meant that the government's role as regulator increases while its role as direct employer decreases. They refer to Majone, [69], who asserts that the regulatory state, rather than public ownership, planning or centralised administration, has arisen as a result of conditions created by privatisation and deregulation. They analyse nine risk regulation regimes, one of which is local road risks, and their analysis is in line with the description of automotive regulation given below. Their analysis of these nine regimes showed that proposed explanations for how the state conducts risk regulation on behalf of their citizens all fail to adequately explain what happens in practice; there are striking variations in risk regulation in different domains and between different nations, for example, what is chosen for regulation and the way that the regulation works. This view is supported by Marcus, [70]. They believe that the changes that the *risk society* seeks to explain can be accounted for by fairly conventional shaping factors, e.g. market processes, pressure groups, historical institutionalism.

Bartle and Vass, [71], highlight the distinction between scientific and social concepts of risk and the differences between public and expert opinions of risk. They are of the view that the adoption of a risk as a *public risk* by the state should not be presumed but rather has to be argued for and justified. They also acknowledge that it is sometimes in the interests of some to keep the public frightened.

Coming from the scientific world, Lewis, [72], looked at technological risk as handled by the many US regulatory regimes. He raises many of the concerns addressed by Hood, Rothstein and Baldwin, [68], and particularly highlights the fact that regimes are intimately bound up with politics, have rules which are mutually contradictory and have boundaries which overlap with other regimes.

Otway and Winterfeldt, [65], note that historically social opposition to technologies was different in each case, and reflected a complex mix of concerns related to: "*morals, religion, political ideologies, power, economics, physical safety and psychological wellbeing*". In contrast, debates today tend to focus on a single issue e.g. risks to public health and safety and to the environment; risk is so significantly at the forefront, that: "*the complex problem of social acceptability is often reduced to a mathematical-numerical problem of defining 'acceptable risk'*". This change has come about to some extent because experts wish to counter negative effects due to enhanced media

coverage of *worst case* scenarios, and examples where experts have covered up embarrassing results, plus the involvement of new environmental organisations, public interest groups and political parties. Consequently, industry and others demanded predetermined criteria by which to judge the acceptability of risks and quantitative risk acceptance criteria were sought. However they criticise the "*... implicit assumption ... that social preferences can be expressed in engineering terms and used in the regulatory process to reduce uncertainty, ambiguity and delay - in essence an attempt to model social and political behaviours with the technical tools and the philosophy of the natural sciences.*" They further note that this modelling approach has been inadequate, as when a numerical approach indicated that the risk was acceptable while in fact there was serious and continuing public opposition.

Otway and Winterfeldt, [65], make many points about how the general population perceive risk in a different way to the experts, based solely on physically measurable parameters, and argue that the risk concept is too narrow to support understanding of the social acceptability of technologies. In particular, they point out that "*'acceptable risk' as a generalizable number or mathematical relationship cannot exist.*". They believe that: "*The acceptance of risks is implicitly determined by the acceptance of technologies which, in turn, depends upon the information people have been exposed to, what information they have chosen to believe, the values they hold, the social experiences to which they have had access, the dynamics of stakeholder groups, the vagaries of the political process, and the historical moment in which it is all happening*". They are in complete agreement that the risks of technology are real and must be managed effectively to ensure public safety, however they argue that it is not sufficient to focus on a single mathematical definition of acceptable risk. There are other *softer* kinds of information which are relevant, and these are held by those people whose lives are affected by the technologies.

Marcus, [70], notes that governments and regulators would like certainty but highlights the difficulty of achieving this by quoting from Weinberg, [73], "*Scientists in their capacity as advisers on problems of technological innovation face particularly troubling dilemmas, as the decisions they make depend on answers to questions which can be asked of science and yet which cannot be answered by science*". He makes the point that in a complex machine it is impossible to identify every possible type of failure; likewise, to build full-scale prototypes to test them under every conceivable circumstance is extremely costly and impractical. This situation means that judgements that have to be relied upon will never carry the weight of a scientific answer, because the underlying issues are on or beyond the limits of what can be scientifically known.

Otway & Wintersfeldt, [65], see that there is a: "*perpetual cycle of regulation and deregulation whereby governments that promote deregulation bring about a return to a risk environment.*". This is brought about because as state intervention is increased due to a systemic crisis or major disaster

the: "*... regulatory control systems tend to produce a political reaction that calls for the dominance of the free market, the reduction of state intervention, a return to liberal values, and the restoration of individual freedoms*".

Quantitative Risk Assessment

The rise of a quantitative approach to acceptable risk, generally referred to as *Quantitative Risk Assessment* or *Probabilistic Risk Assessment*, is described by Covello and Mumpower in [74]. They describe how probability has been used to establish causality relating to ill health (epidemiology) from the sixteenth century onwards, while it has only been used to predict failure rates for man-made artefacts since World War II. The American Atomic Energy Commission first looked at quantitative risk assessment for radioactive release in 1957. In 1975 the first modern quantitative risk assessment for reactor safety was published. Although much criticised at the time, the approach became the norm after the Three Mile Island incident in 1979, [58]. NASA started looking at the use of numerical values for the probability of mission failure and death or injury per mission in 1969 and *Quantitative Risk Assessment (QRA)* became standard practice after the loss of the Challenger Space Shuttle in 1986, [58]. The use of QRA for chemical plants was pioneered by the Dutch and dates from the Post Seveso EEC Directive of 1982, which required each member state to develop a risk management methodology, [58]. The use of *Probabilistic Risk Assessment* (PRA) has been strongly criticised by Leveson, [75].

Renn, [76], says that risk can be framed in different ways depending on the perspective taken: technical assessment of risk; economic, psychological, and sociological assessment of risk; public perception of risk; risk used as a trade-off criteria; and risk used to design resilient strategies for coping with remaining uncertainties. He also notes that while technical assessment may provide the best estimate for the probability of an event, public perception should be the basis for deciding acceptable or tolerable risk.

Aven, [77], comments that there are a number of prevailing perspectives on risk: engineering approaches; economic, decision-oriented perspectives; social science perspectives; and anthropology perspectives. He recognises the difficulty, when making a decision related to risk acceptability, of assessing the public's view, [78], and also the problems of letting professionals make the decision, [79].

Grafjodi, [80], notes that the public perception of risk depends on other culture norms, the frequency or rarity that individuals witness or are involved in accidents and the degree to which exposure to the risk is voluntary. There is also the natural aversion of people to severe consequences, e.g. large number of fatalities, from a single incident, known as *differential risk aversion*.

Aven, [81], has noted that, even within what might be considered to be the technical perspective, there are many different definitions of risk. He notes nine different ones all constructed from one or more of: expected value (loss), probability (of an undesirable event), objective uncertainty, uncertainty, event/consequence, potential/possibility (of a loss), and uncertainty on objectives. Some definitions only consider the possibility that an adverse outcome may occur, some only consider the severity of the outcome while others consider both. It is the last of these which is usually used in an engineering context.

Whereas it can be seen that socially acceptable risk does not exist in any meaningfully quantifiable way, papers coming from the engineering and science background pre-suppose that it does. Aven, [78], who after having used it as a parameter, says that there are no strict limits on what is socially acceptable. There are differences of opinion, sometimes extreme, for example among politicians; there is also disagreement among experts. Aven, [64], also notes that when risk acceptance criteria are formulated by the plant operators this does not generally serve the best interests of society as a whole. He concludes that it is preferable for the authorities to formulate the risk acceptance criteria.

Probability

We see from the above that notions of acceptable risk are fraught with difficulties. While the general public, and those in authority, would like decisions to be based on undisputed scientific fact, it is recognised that such firmness in the underlying data still eludes us. As noted, most definitions of risk involve the possibility that an adverse outcome will occur. There are differing views on how the 'possibility' of an adverse outcome should be captured. Probability is often used as the underlying concept. There are different interpretations of probability; the two main schools are often referred to as *frequentist* and *Baysian* (also called *subjective*), [82]. Although the mathematics is the same in both cases the underlying philosophy is different. The *frequentist* approach assumes that there is an objective value of probability for some event which exists in the universe independently of people, while the *Bayesian* approach takes the value of probability to a measure of personal belief rather than a property of the world, Aven, [81]. All schools of probability are attempting to deal with uncertainty which is often classed as either aleatory or epistemic, [58]. *Aleatory uncertainty* is used for those circumstances where the uncertainty is due to the stochastic nature of the world and as such is considered to be inherent and thus irreducible. *Epistemic uncertainty* is used for those circumstances where the uncertainty is due to a lack of knowledge and in principle further exploration would produce more knowledge which in turn would reduce the uncertainty. Aven, [83], links the *frequentist* understanding to *aleatory uncertainty* while the subjective *Baysian* approach he links to *epistemic uncertainty*. To some extent *epistemic* is often treated as if it is *aleatory* because it is just too difficult and requires too much effort to reduce the *epistemic uncertainty*.

Cohen, [84], has quite a different take on probability. He is critical of previous formulations and states that they are not applicable in all circumstances. He takes legal systems as an example. They use probability because in a civil case it has to be decided on the *balance of probabilities*. Cohen makes the point that the amassing of circumstantial evidence is considered to increase the likelihood in favour of the *balance of probabilities*. However, if a standard mathematical approach was used, each piece of circumstantial evidence would have a probability value and to process the conjunction of the evidence the probability values would be multiplied together. As each value of probability is less than one the result would be smaller than any of the originals. Thought of in this way, the more evidence that was presented the less strongly the case would be made. This is clearly not how the court sees it, so its concept of probability is different from the standard mathematical one. It is not obvious how to apply this in an engineering context, although Weinstock, Goodenough and Klein, [85], suggest it may have a role to play in the context of safety cases.

Taleb, [86], has also argued that a probabilistic approach is not appropriate for predicting rare events which have a significant impact. These types of events he refers to as *black swans*. Interpreting this in a risk context, Aven, [87], suggests that it is most appropriate to think of a *black swan* as an extreme, surprising event relative to the present knowledge rather than a rare event with extreme consequences. In [88] he proposes a new risk perspective which adds *surprises* (*black swans*) to the elements of probability-based-thinking and knowledge-dimension which he had discussed at length in other papers.

Legal Considerations

The state exercises its will through either the civil or criminal law, [89]. The civil law is used to compensate victims of faulty products. The 1987 Consumer Protection Act, in the UK, brought together the previous piece-meal legislation with a general requirement that *consumer goods* comply with a catch-all *general safety requirement*, but the act does not give any details of what constitutes the *general safety requirement*. Where appropriate standards exist, a manufacturer will seek to meet the *general safety requirement* by complying with the standard because they know that a court of law will accept this as being a statement of best practice. The criminal law is intended to prevent faulty products being sold; it also encourages manufacturers to rectify goods found to be faulty, and perform recalls if necessary, as a way of reducing penalties imposed by the courts.

Sociological view of risk summary

Risk is seen as a human construct and there is no absolute concept for it. The general public are not sympathetic to a probabilistic definition and there is also debate in the engineering community about defining risk this way and then using probabilistic design targets. The concerns of the public change over time, and there is a disconnect between public perception and the engineering view and

treatment of risk. The state attempts to bridge this gap by creating legislation, with the aim of reassuring the public, while leaving the details to the engineering community.

2.2.2 Industrial Regulations and standards

As mentioned previously, there are several different aspects of risk regulation. The regulations, or regulatory guidelines, could be written at the international level or at the national level. If the latter, then there is the nature of the relationship between international and national material. The regulations, or regulatory guidelines, may specify performance targets; they may include certification requirements together with requirements for achieving certification. Performance monitoring may also be included.

In this section we review the regulations and standards of a number of industrial uses of *mechatronic* systems. Our main focus is on vehicles excluding trucks and buses.

Railways

The public only come into contact with this equipment via the companies that operate the rail network containing or using the equipment and there are a large number of supplier companies that produce the individual pieces of equipment.

Railways are mainly governed nationally, but in April 2004 the European Railway Agency (ERA), [90], was set up to create a competitive European railway area by increasing cross-border compatibility of national systems, and in parallel ensuring the required level of safety. In the main, the regulators are Government agencies. A yearly performance report is produced by the European Railway Agency, [91], which reports fatalities against *Passengers*, *Employees*, *Level-crossing users*, *Unauthorised persons* and *Others*. Fatalities are dominated by *'unauthorised persons'* and '*levelcrossing users'*. There is no direct correlation between equipment failure and this data.

Railway operators are required to have a safety management system, and the mainline railway should include targets related to the European Common Safety Targets set for the member state, [92]. The EU requires that risks in the following categories be assessed as a number of passenger Fatalities and Weighted Injuries (FWSIs) per year:

- Risk to passengers
- Risk to employees
- Risk to level crossing users
- Risk to 'others'
- Risk to unauthorized persons on railway premises
- Risk to the whole society

These are to be judged against a national reference value (NRV). The intention is to derive common EU safety targets (CSTs) from the NRVs, [93]. There is also a European requirement to adopt a common safety method on risk evaluation and assessment, [94]; this specifies a process but does not give the details of how to assess risk or decide if the risk is acceptable. Instead there are many references to national and European documents.

The CENELEC norms EN 50126, [95], EN 50128, [96], and EN 50129, [97], are obligatory standards for European countries. EN 50126 defines a systematic process for specifying requirements for reliability, availability, maintainability and safety (RAMS) and demonstrating that the requirements have been achieved. The EN 50128 specifies procedures and technical requirements for the development of software and the interaction between software and the system which it is part of. The EN 50129 specifies lifecycle activities to be completed before the acceptance stage, followed by additional planned activities to be carried out after the acceptance stage. It is closely related to the EN 50126, [98].

Civil Aircraft Avionics

Again, the public only come into contact with this equipment via the aviation companies that operate the planes containing the avionic equipment. The government bodies act as the regulators, assessors and certifiers. The top-level regulator for civil aviation is the International Civil Aviation Organization (ICAO), an agency of the United Nations, established by the Chicago Convention in 1944, [99]. It sets international standards that national authorities have to follow. Different national or international bodies exist, e.g. US Federal Aviation Authority FAA, [100]. European regulation is increasingly coming under the remit of European Aviation Safety Agency (EASA), [101], created in 2002, instead of the national authorities such as the Civil Aviation Authority (CAA) in the United Kingdom (UK) and the Direction Générale de l'Aviation Civile (DGAC) in France. In the US, requirements are issued as Federal Aviation Regulations (FARs) and in Europe as Joint Airworthiness Regulations (JARs). Minimum performance standards are specified by the issuing of Technical Standard Orders (TSO). Targets for reductions in aviation fatalities are set by government bodies.

The following documents are normally considered to be the relevant standards but in practice their legal status is of guidance which RTCA defines as: "*material that could be recognized by the authorities as a means of compliance to the regulations*", [102].

- ARP4761 Guidelines and Methods for Conducting the Safety Assessment on Civil Airborne Systems and Equipment, [103]
- ARP4754A/ED-79A Guidelines for Development of Civil Aircraft and Systems, [104]
- DO-178C/ED-12C Software Considerations in Airborne Systems and Equipment Certification, [105]

- DO-254/ED-80 Design Assurance Guidance for Airborne Electronic Hardware, [106] ARP4754A/ED-79A, DO-178C/ED-12C and DO-254/ED-80 are all objective-based. They do not prescribe any particular system, software or hardware processes or lifecycles. Rather, they describe the objectives that the chosen system, software or hardware lifecycle has to satisfy.

It is a common misconception that FAR 25 requires that avionic software has to demonstrate a failure rate of 1×10^{-9} failures per hour or less. FAR 25 states that the aeroplane systems must be designed so that: "*the occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable*". FAR 25 does not mention software, nor does it define "*extremely improbable*". Advisory Circular AC 25.1309-1A (FAA 1988) describes various acceptable means for showing compliance with FAR 25.1309. These means are not mandatory. AC 25.1309-1A suggests that, when using quantitative analyses, extremely improbable failure conditions should be considered to be those having a probability on the order of 1×10^{-9} or less, [107].

The use of QRA in aircraft certification tends to be restricted to the use of techniques such as *Fault Tree Analysis* (*FTA*) and *Failure Mode Effect Analysis (FMEA*) to calculate the effect of random hardware failures such as component wear-out.

Medical Devices

These devices are worn by the patient. Currently most devices are fitted by medical staff but this may change in the future as more publicly available devices come on to the market.

The Medicines and Healthcare Products Regulatory Agency (MHRA), [108], is responsible for regulating all medicines and medical devices in the UK by ensuring they work and are acceptably safe. The MHRA also includes the National Institute for Biological Standards and Control (NIBSC), [109], and the Clinical Practice Research Datalink (CPRD), [110]. The MHRA is an executive agency of the Department of Health.

Manufacturers wishing to make an application for pre-clinical assessment of a proposed clinical investigation of an active implantable medical device or a medical device to be carried out in part or in whole in the UK have to apply to the MHRA in accordance with specified guidance notes [111] which calls up ISO 14971, [112]. This has requirements for hazard and risk assessment but does not provide a common risk assessment or mitigation scheme, requiring each company to decide for themselves. It also makes no mention of development process measures for hardware and software.

Nuclear

In the US regulation is performed by the Nuclear Regulatory Commission (NRC), [113] which is an independent agency of the United States government. The European Nuclear Safety Regulators Group (ENSREG), [114], is an independent, authoritative expert body created in 2007 following a decision of the European Commission. It is composed of senior officials from the national nuclear safety, radioactive waste safety or radiation protection regulatory authorities and senior civil servants with competence in these fields from all 27 Member States in the European Union and representatives of the European Commission. ENSREG's role is to help to establish the conditions for continuous improvement of safety and to reach a common understanding in the areas of nuclear safety and radioactive waste management.

The Office for Nuclear Regulation (ONR), [115], is the designated UK Nuclear Regulatory Authority responsible for regulating safety and security. ONR is an agency of the Health and Safety Executive (HSE) pending relevant legislation to create ONR as a statutory corporation. ONR brings together the safety and security functions of HSE's Nuclear Directorate (incorporating the Nuclear Installations Inspectorate, Civil Nuclear Security and the UK Safeguards Office) and from summer 2011 the Department for Transport's Radioactive Materials Transport division.

In the UK, the Health and Safety Executive publishes the *Safety Assessment Principles for Nuclear Facilities (SAPs)*, [116], which apply to the assessment of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other duty holders. In paragraph 529 it states that:

- "*Probabilistic Safety Analysis should assist the designers in achieving a balanced and optimised design, so that no particular class of accident or feature of the facility makes a disproportionate contribution to the overall risk, e.g. of the order of one tenth or greater. PSA should enable a judgement to be made of the acceptability or otherwise of the overall risks against the numerical targets and should help to demonstrate that the risks are, and remain, ALARP.*"

In paragraph 599 it sets targets for the effective dose received by any person arising from a design fault for both onsite and off-site persons. This is the clearest setting of risk targets of any of the industrial domains considered.

The US recognises three levels of *Probabilistic Risk Assessment*, [117]:

- Level 1 PRA estimates the frequency of core damage. It starts with conditions that are well known, usually with a reactor operating at full power. All of the systems that work to protect the reactor are modelled. Since the workings of these systems are well understood, the uncertainty of the result is relatively small.

- Level 2 PRA estimates the magnitude and timing of releases. (That is, "*Assuming that the core is damaged, how much radioactivity might escape into the environment?*") Uncertainty associated with how much coolant escapes the reactor systems (and how violently), as well as variation in containment system response, makes a Level 2 PRA less precise than a Level 1 PRA.
- Level 3 PRA assesses the injuries and economic losses that might result if radioactivity escaped from containment. Highly variable factors like wind speed and direction will affect the results.

However, a report written in 2012 proposing a risk management regulatory framework, [118], found that: "*The concept of design-basis events and accidents continues to be a sound licensing approach, but the set of design-basis events and accidents has not been updated to reflect insights from power reactor operating history and more modern methods, such as probabilistic risk assessment (PRA)*" and recommended that: "*The set of design-basis events and accidents should be reviewed and revised, as appropriate, to integrate insights from the power reactor operating history and more modern methods, such as probabilistic risk assessment (PRA).*" This implies that although PRA has a long history of use in the nuclear industry it is not as central to the licensing requirements as it could be.

While regulating safety is a national responsibility, international standards and harmonized approaches to safety promote consistency and help to provide assurance that nuclear and radiation related technologies are used safely. The International Atomic Energy Agency (IAEA), [119], is required by Statute to promote international cooperation and for over fifty years has published more than two hundred safety standards which reflect an international consensus on what constitutes a high level of safety for protecting people and the environment. The principal users of the safety standards are regulatory bodies and organisations that design, manufacture and operate nuclear facilities but they are not binding on states and are used in different ways in different countries. They are applicable, as relevant, throughout the entire lifetime of all facilities and activities, existing and new.

Within the UK, the IAEA Safety Standards were used to benchmark the recent review of SAPs, and in the continuing review of the Technical Assessment Guides (TAGs), [115]. The Safety Standards were also used by the Western Nuclear Regulators Association (WENRA) in deriving their reference levels, [119].

Automotive

In the main, the product is owned and operated by members of the general public although vehicles are also hired and leased. In the automotive domain there is government direction pertaining to both the sale of individual vehicles and to targets, or aspirations, for road traffic accidents as a whole.

Road safety targets, or aspirations, are often expressed as relative reductions in terms of road deaths or those *Killed or Seriously Injured* (KSI), [120]. They may be set at international and national level. The United Nations General Assembly has proclaimed the period 2011-2020 as the *Decade of Action for Road Safety*. Their goal is to stabilise and then reduce the forecast level of road traffic fatalities around the world. They hope to do this by conducting activities at the national, regional and global levels related to five pillars, namely: road safety management; safer roads and mobility; safer vehicles; safer road users and post-crash response. They list ten reasons to act based on the number of people killed or injured (90% of these injuries occur in developing countries), the direct and indirect costs to the economies and the fact that: "*Road crashes are preventable*", [121], [122].

A hundred governments, including the UK, have co-sponsored the UN resolution establishing the *Decade of Action* and committing themselves to work through an *Action Plan* with targets for raising helmet and seat belt use, promoting safer road infrastructure and protecting vulnerable road users, such as pedestrians and cyclists, [123]. Note, vehicle defects of the type that this thesis is concerned with are not included.

The focus on achieving these is on the driver because this reflects the common understanding, based on the data currently available, that it is the driver who is directly responsible for most accidents, [120], [7]. Road infrastructure is a significant, but much smaller, contributing factor and vehicle defects make a very small contribution. A 2010 report from the Institute of Advanced Motorists covering 2005 - 2009, [124], assigned the road environment as being a contributory factor in 15% of all road traffic accidents and vehicle defects as a contributory factor in 2% of them. The UK 2011 Annual Report for reported road casualties, [125], placed vehicle defects as the smallest contributory factor. Ellims, [126], argues that very few of these will be the result of software defects.

This understanding is used as the rationale for moving more and more towards driverless vehicles; [6], it remains to be seen if this will yield the hoped for results. It is observed that when all vehicles are driverless then all accidents will be the result of vehicle defects. In 1987 the UK government set its first target of reducing road accident casualties by a third by the year 2000. The actual result was that fatalities and serious injuries had fallen by a third, but there was an overall rise due to an increase in slight casualties. In 2000 targets were set for 2010. These were based on what was thought possible by addressing alcohol consumption, road safety engineering and secondary safety. The targets, against a baseline of a 1994 to 1998 average, were set as a 40% reduction in KSI, a 50% reduction in children KSI and a 10% reduction in slight casualties per 100 million vehicle kilometres, [127].

The UK response to *Decade of Action for Road Safety* is contained in *Framework for Road Safety*, [3]. Responsibility is devolved down to local authorities and no national targets for reductions are given, a decision that was criticised by RoSPA (Royal Society for Prevention of Accidents), [128].

The main focus is on addressing driver failings; other factors also known to contribute to road accidents, such as the road infrastructure and vehicle defects, are not mentioned. The report says that performance against the indicators in the Road Safety Outcomes Framework will be monitored and anticipates that: "… we could see fatalities falling by around 37% … by 2020" and a "Killed or Seriously Injured …reduction of 70% by 2030". The report acknowledges the rapid development of advanced safety systems, and ones with good safety potential; these include advanced emergency braking systems, lane departure warnings, and blind spot warnings. It also acknowledges that other new technology may affect driver workload in terms of distraction or detachment from the driving task. The change in emphasis in this from the target setting of 2000 probably reflects a different political philosophy.

An example of a response to this devolved responsibility is that of Kent, [123], whose approach is broader than that of the UK government, being based on:

- influencing the road user (through Education, Training and Enforcement);
- the road environment (through Engineering);
- the vehicle (through working with Manufacturers) in combination with a range of practical measures to continue to deliver reductions in road casualties.

Each nation determines for itself what regulations apply for the sale of motor vehicles and the means by which the regulations are enforced. There can be hundreds of different regulations for one vehicle with differing versions in different markets. However, there is much cooperation between nations and cross-acceptance of each other's regulations. There is ongoing work towards global harmonisation of regulations, [129]. In the main, regulations apply to components or systems although there are some whole vehicle regulations, e.g. electromagnetic compatibility. The acceptance criteria are based on tests prescribed in regulations; there is little analysis of design and the criteria are not based on failure rates, [2].

Most regulations are not directly related to safety concerns, although some are, for example steering [130]. The means of enforcement differ. In many countries, including those which are members of the European Union, vehicles have to be certified before they can be sold. The certification prior to sale is performed by public or private agencies; this is the Vehicle Certification Agency, VCA [131], in the UK. In other countries, e.g. the US and Canada, the vehicle manufacturers self-certify. The government agencies, National Highways Traffic Safety Administration, NHTSA [132], in the US sample vehicles for compliance.

Regulations are made concerning both the manufacture of vehicles and the licensed use of vehicles on the public highway. The former are technical, with details being provided by technical people rather than by governments. The latter are seen as the major source of accidents and this view is supported by the data. With such a low percentage of accidents being attributed to vehicle defects,

it is not surprising that no attempt is made to link road accident reduction targets, or aspirations, to the contribution of the legislative regulations.

Where the vehicle itself is concerned, previously the emphasis was on severity mitigation, helping the vehicle occupants to survive crashes. Now, greater emphasis is being placed on preventing the accidents; it is argued that this can be achieved by using *Advanced Driver Assistance Systems (ADAS)* to provide more information to the driver and progressively take actions on behalf of the driver to prevent collisions, [133]. As mentioned above, the long-term goal is to move increasingly to autonomous vehicles which tend to be seen as safe by definition as there is no longer a driver, [6].

The only automotive functional safety standard, ISO 26262, [13], acknowledges, that with the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures and so it includes guidance to avoid these risks by providing appropriate requirements and processes. It is not a legal requirement, i.e. it is not part of any regulations that must be met to sell the vehicle. It is followed as a statement of best practice which would form the basis of any defence in a product liability case. There is also the *Code of Practice for the Design and Evaluation of ADAS*, [134], which summarises best practices and proposes methods for risk assessment and controllability evaluation. It pre-dates ISO 26262 but has essentially the same risk assessment scheme. Again, this document is not a legal requirement and only serves to provide a benchmark for what can be considered to be best practice.

The scope of the risk addressed in ISO 26262 is limited to: "*failure or unintended behaviour of an item with respect to its design intent*". The term *item* is defined as system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied. When work began in Germany on what was to become the standard, the intention was to cover the automotive electronic control systems that were current at that time, but during the course of the eleven years that it took to reach publication, the standard sought to address: "*the trend of increasing technological complexity, software content and mechatronic implementation*".

Like IEC 61508, [135], ISO 26262 is based around a safety lifecycle that starts with identifying *hazards* and covers development, manufacture, service and disposal, although in practice the last three are not covered in any depth and do not generate any significantly new requirements.

The standard requires that hazards associated with the *item* being developed are identified and their unmitigated risk assessed. The risk scale starts with *Quality Management (QM*) for which the remainder of the standard is not applicable, and then proceeds through a series of *Automotive Safety Integrity Levels* (ASILA, ASILB, ADSILC and ASILD), as the assessed unmitigated risk increases. This automotive standard seems to be unique among the sectors in providing a single risk assessment scheme for all vehicles in the scope of the standard. However, using the risk assessment

scheme involves making subjective judgements which could lead to different risk assessments for similar items. Practical experience is showing that in the main this is not happening.

ISO 26262 seeks to avoid *unreasonable residual risk*. The fact that the standard does not apply to hazards classified as *QM* implies that unreasonable residual risk can be avoided by the application of standard automotive quality management practices, including the failure mode avoidance practices. For each hazard not classified as *QM*, a *safety goal* has to be defined, which if met, achieves freedom from *unreasonable risk*.

Current *safety goals* are usually defined around ensuring that vehicle control can be maintained by the driver. This correlates well with the 1968 Vienna Convention on Road Traffic, [136], which requires that: "*Every moving vehicle or combination of vehicles shall have a driver*." and that: "*Every driver shall at all times be able to control his vehicle …*". This convention will need to be changed in order for driverless vehicles to be allowed on the road. There are moves within Europe to amend the convention in this way.

From the *safety goals*, a succession of safety requirements are progressively derived: *functional safety requirements*, *technical safety requirements*, *hardware safety requirements* and *software safety requirements*.

Assurance that the *safety goal* has been met is gained by meeting the standard's recommendations for system, hardware and software development process measures and its recommendations related to hardware reliability and diagnostic coverage. The standard also says much about general engineering issues such as planning, document control and tools.

The requirements of ISO 26262 to achieve freedom from unreasonable risk contain a lot of leeway and allow many different solutions, for example:

- There are no explicit criteria against which the adequacy of the top-level safety requirements, *safety goals*, can be judged;
- A large amount of discretion is allowed in deciding which development process measures to use;
- The requirements related to random hardware failures and diagnostics coverage allow significant variation in the setting of targets and the means by which a design target can be shown to have been met.

A fuller exposition of ISO 26262, covering risk assessment, safety requirements, integrity and functional safety assessment is given in Appendix B.

The scope of ISO 26262 is limited to malfunctioning behaviour against design intent. A new document giving guidance for how to define functionality that is considered safe is being prepared and is due for final publication in 2018, [137].

Regulations and Standards Discussion

The nuclear, railways, civil aviation and medical devices sectors are strongly regulated whereas the automotive sector is less regulated, for example in some markets the vehicle manufacturer performs self-certification. This may be because the strength of the regulations is related to the extent to which those affected have any ability to control the risk and also the number of people exposed to risk as a result of a failure event. In the automotive sector the vehicle is owned and used by members of the public, so they inherently have to take some responsibility. The other sectors are run by *professionals* on their behalf and the public has no role and consequently no responsibility. The process for the harmonisation of automotive regulations is as much driven by a desire to promote trade as it is to ensure common standards, most of which are not directly related to safety concerns.

The railways sector has the most similarity to the automotive sector in terms of the interaction of the public with the machine and their exposure to the associated risk. In the rail industry, the many different ways that people are exposed to risk are considered individually because the means to achieve risk reduction may be different in each case. There is no equivalent for automobiles as, to date, improving driver performance is seen as the major was of reducing risk associated with the automobiles. Railway companies are required to operate a safety management system; there are no such requirements for automotive companies. It is common practice to conform to quality management requirements, e.g. TS16949, [138]. It is also common practice to have a process that specifically responds to in-service incidents that are safety-related.

All sectors have safety standards and in most sectors there are efforts to have common ones in different jurisdictions. The civil avionics standards, while mentioned in regulations, are not a formal regulatory requirement. This is similar to the situation with ISO 26262, which is not yet mentioned by any piece of regulation. ISO 26262 is more prescriptive than the civil avionics standards, although it attempts to be goal orientated in places by allowing quite a lot of discretion in how the goals are achieved. Like ISO 26262, the railway CENELEC standards are based on the generic IEC 61508, but unlike ISO 26262, they are a regulatory requirement. The medical devices sector appears to have the weakest standards.

The nuclear industry is alone in prescribing the use of *Probabilistic Safety Analysis*. Their situation is quite different to the other domains considered here in having just one plant with a fixed environment. While the risk is known and fairly constant, those potentially exposed to it include employees and near neighbours as well as national and international geographic areas. ISO 26262 uses numbers for assessing hardware reliability and diagnostics coverage, but they are not used as a key target of the standard; there is much discretion left to the developer about what targets to set and how to show they have been achieved, e.g. a target may be: "*derived from the hardware*

architectural metrics calculation applied on similar well-trusted design principles". While civil avionics has a well-known target for hardware failures, it is not in practice a regulatory requirement.

2.2.3 Risk Summary

From an engineering perspective it is necessary to meet standards, either because they are required by regulations or represent best practice from a product liability perspective. As we have seen, these are not necessarily in good alignment with the view of the general public. When performing risk assessment, in accordance with a process given in a standard, there are many subjective judgements that have to be made, so it is well to bear in mind the potential gap between the engineering handling of technical risk and the public perception of those risks. Having acknowledged that, working within the limitations of standards, e.g. ISO 26262[13], still provides a good base for the work on a *mechatronic system* safety argument.

2.3 Product Assurance - Industrial practice

We first provide an historical overview of quality control and management before reviewing how this is applied to product quality. We then review how safety has been addressed in mechanical engineering before considering the more recent development of functional safety.

2.3.1 Quality

By the start of the 20th century the use of standardised interchangeable parts in manufacturing had become common. This increased the repeatability in the manufacturing process and opened the way for a probabilistic treatment. In the 1920s, Dr. Walter A. Shewhart at Bell Labs pioneered the use of statistical quality control for product improvement and in1931 he published *Economic Control of Quality of Manufactured Product*, [139], and set the founding principles of quality control.

Quality Management systems grew out of the defence industry's need to move away from quality control by inspection to quality assurance based on a demonstration that their suppliers' processes were both effective and under control and that there was effective control over procedures and systems [140]. The global standard for quality management systems is ISO 9000, first published in 1987. This has its origins in the British Standards Institute's quality standards BS 5750. The latest version was published in 2015, [141]. The standard requires clear and specific documentation of policies, procedures and work instructions. There are six required quality policies and procedures: Document Control, Control of Quality Records, Control of Non-Conforming Product, Corrective Action, Preventive Action and Internal Audits. In 1994 a version of ISO 9000 was created specifically for the automotive industry, QS9000, [142]. This was widely used until 2006. It has now been replaced by IATF 16949:2016, [143], which itself superseded the earlier ISO/TS 16949, [138]. ISO 9000 has also been applied to software development. In 1997 ISO issued ISO 9000-3, [144], under the name of TickIT, this has now been superseded by TickIT*plus*, [145]. A common

software quality framework used with the automotive industry is Automotive SPICE®, [146], derived from ISO 15504, [147].

While quality management systems address the design and manufacture of a product, *Total Quality Management (TQM)* seeks to address all aspects of the business, including the quality control and quality assurance, [140]. It is an umbrella term that encompasses many product and quality initiatives. One such initiative is *Six Sigma*, originating from Motorola in the 1980s. This is a methodology to improve product or a service process provided to outside customers by increasing performance and decreasing performance variation. The name *Six Sigma* derives from statistical terminology where sigma means standard deviation. For normal distribution, the probability of falling within a ±6 sigma range around the mean is 0.9999966. The intent of *Six Sigma* is to reduce variation so as to achieve very small standard deviations. This is accomplished by the DMAIC process (define, measure, analyse, improve, control) for improving existing processes and the DFSS (design for six sigma) process to develop new processes or products at *Six Sigma* quality levels, [148].

2.3.2 Product Quality

As mentioned above, the first approaches to product quality was quality control by inspection. Fuelled by the large scale use of electronics starting in World War II, mainly vacuum valves, [149], there was a move to predicting failure rates of equipment, based on component failure rates, and then setting target values for equipment failures in the field, [150]. Also, at this time a number of reliability societies and journals were established. Reliability engineering remains a major technique in product development, [151], [152], including electronics, [153].

Components are characterised by simple failure models based on what is physically possible. For electronic technology this includes resistors, capacitors, field effect transistors and integrated circuits, although the last of these has a very complex internal structure. As the failure model is simple, the main source of uncertainty is aleatory, relating to when a component will fail. For this circumstance a probabilistic approach to predicting failure rates has been shown to be accurate over many years of successful use, [154], [155]. The previous performance of a large population of components can be taken to be a good indicator of the future performance of a similar population provided that the two populations are assumed to have the same properties. This assumption is normally justified on the basis of a common and controlled manufacturing process. In assessing the failure rates local environmental factors, e.g. temperature, also have to be accounted for and so the assessment must be made under a typical operational and environmental profile. Generic tables are available that give failure rate data for electronic components; these have wide acceptance in many industries and are generally judged to be on the conservative side, [156], [157]. Problems may arise in obtaining the basic figures. Aven, [158], highlights that lack of relevant component reliability

data is a problem in many reliability analyses. Often new components are used in the design and so the predicted performance is based on an assumption that the failure properties of new component will be similar to those assessed for an established component. With assemblies of components the failure modes are no longer be generic but particular to the design. Therefore, a failure model has to be constructed and, particularly for an assembly of assemblies, may get quite complex. It may be modelled explicitly by constructing a fault tree, [58], [154], or just be implicit in a Failure Mode Effects Analysis (FMEA), [159], [160]. The more complex the failure model, the greater will be the epistemic uncertainty associated with it. The failure model uses the failure data of the components of the assembly, each of which brings with it its aleatory uncertainty.

Another approach to reliability is Physics of Failure, [161], [162], [163]. This seeks to understand why failures occur in terms of the fundamental physical and chemical behaviour of the materials out of which the components are made. Such understanding can then be used to eliminate the failures or provide more accurate formulations reliability models. This is in contrast to the more empirically-based reliability prediction approaches. The advocates of Physics of Failure believe that while the analysis is complex and costly to apply, it provides the strongest characterization available of reliability of components, structures and systems. By the early 1960s there were then two approaches to reliability; one a quantitative approach based on predicting failure rates and the other based on identifying and modelling the physical causes of failure.

There has been much debate about whether or not reliability can be applied to software. Perhaps the most common view is that software is purely a design and as such does not fail in the way that a physical component can fail. Therefore, a probabilistic approach is not appropriate. This is the view of all the safety standards, e.g. IEC 61508, [12], that clearly state that the probabilistic targets do not apply to software. This common view has been challenged by staff at City University and the Centre for Software Reliability, [164], [165]. Their view is that the uncertainty in software failure is a result of the randomness in the inputs to the software and that this can be represented probabilistically.

In the automotive industry there has been a move away from basing quality on reliability due to the difficulty of obtaining accurate field performance figures given that there is large uncertainty concerning the nature of the environment in which the product will be used. Brown, [166], highlights the problem of knowing the stated conditions and specified period of time which would have to take into account the field usage, speeds, loads, duty-cycle of loads, temperature dynamics, humidity, corrosive environments and shock loads. Davis, [167] highlights the lack of closed-loop feedback from units in the field when data outside the warranty period is not collected.

Given these criticisms an approach, known variously as Robustness Engineering or Failure Mode Avoidance (FMA), has been adopted. Robustness is also a part of TQM and Six Sigma and has its

roots in the work of Taguchi, [168]. Taguchi defines robustness as the "*state where the technology, product, or process performance is minimally sensitive to factors causing variability (either in the manufacturing or user's environment) and aging at the lowest unit manufacturing cost*". Robustness recognizes two types of quality: customer quality, i.e. features the customer wants, and engineered quality, i.e. features the customer does not want. Robustness is about engineered quality, i.e. removing the features that the customer does not want such as failures, noise, vibrations, unwanted phenomena and pollution. It does this by identifying the *ideal function* and then selectively choosing the best nominal values of design parameters that optimise performance reliability at lowest cost. The classical metrics for quality/robustness, e.g. failure rate, are considered to come too late in the product development. The Taguchi measure for robustness is signal-to-noise ratio. The signal-to-noise ratio measures the quality of energy transformation as expressed by the ratio of the "*level of performance of the desired function"* to the "*variability of the desired function"*. The signal-to-noise ratio is increased by reducing variability and specifying nominal values of the design parameters such that the design is insensitive to noise factors, e.g. the customer environment, aging and wearing, and manufacturing variations.

Clausing, [169] has suggested a new definition for reliability: "*reliability is failure mode avoidance*", with failure being any customer perceived deviation from the ideal condition. As reliability is being equated to failure mode avoidance it is necessary to a have a way of measuring it. Clausing proposes the "*operating window*", (OW) as a metric for robustness. The OW is the range in some input noise that produces a fixed failure rate in the failure modes. Davis, [167], accepts Clausing's view of reliability as failure mode avoidance and proposes a robustness metric called the "*distance from the failure mode*". The distance is captured as measurements of physical properties in SI units, the greater the distance the higher the reliability. Campean *et al*, [170], [171], also agree with Clausing and Davis that: "*reliability is failure mode avoidance*".

Failure Mode Effects Analysis

Failure Mode Effects Analysis (FMEA) is a technique that is used extensively by the quality, reliability, robustness and failure mode avoidance disciplines. There are a number of standards for FMEA, including SAE J1739, [159], VDA *Product- and Process-FMEA*, [172], and IEC 60812, [160]. J1739 and the VDA guide are commonly used in the automotive industry. Use of FMEA is called for by IATF 16949:2016, [143], which is the universally used quality standard in the automotive industry. An FMEA may be performed on a process or a product; here, we are only concerned with the analysis of a product, which is often referred to as a design FMEA (DFMEA).

The primary purpose of the FMEA is to identify potential high risks and keep them from occurring in the end product, or minimize their effect on the end user. Three means are used: changing the

design, preventing the risk from occurring, or detecting the risk before production. Risk in this context is mainly concerned with quality issues, with only the highest severity effects being related to the safe operation of the vehicle, see below.

The description of the FMEA given here is largely taken from J1739 which describes the procedure for a DFMEA in terms of the data produced when performing the technique, see Table 2.

The *item* is represented as a set of *functions*. For each *function*, the *effect* of it experiencing a number of *failure modes* is considered. Typical *failure modes* considered include: loss of function, partial function, intermittent function, degradation and unintended function. It is normal to consider what the *effect* will be at the boundary of the *item* and also at the final product level. Each *effect* is assigned a *severity ranking*, 1 to 10, and the severity of the *function failure mode* is taken as the highest ranking value from all of its *effects*. The ranking is relative within the scope of the individual FMEA and is determined without regard to the *occurrence ranking* or the *detection ranking*. A *severity ranking* of 9 or 10 is typically assigned if the effect is considered to affect the safe operation of the vehicle. The *severity ranking* cannot be changed without eliminating the *failure mode* and its *effects*.

Data Item	**Description**
Item	The name or other pertinent information of the item being analysed.
Function and Requirement	Function is a description of the design intent for a system, subsystem, or component. Product requirement defines how a product function should perform.
Potential Failure Mode	The manner in which a component, subsystem, or system could potentially fail to meet or deliver the intended function(s) and its requirements.
Potential Effects	Consequences or results of each failure mode.
Severity Ranking Number	Relative ranking within the scope of the individual FMEA for the most serious effect for a given failure mode for the function being evaluated.
Classification	Optional means to highlight failure modes or causes for further action.
Potential Cause of Failure	Indication of how the failure could occur.
Occurrence Ranking Number	Relative ranking within the scope of the individual FMEA for the likelihood that the cause will occur during the design life of the product.
Current Design Controls – Prevention	Description how a cause, failure mode or effect is prevented.
Current Design Controls – Detection	Description how a cause and/or failure mode is detected, either by analytical or physical methods, before the item is released to production.
Detection Ranking Number	Relative ranking within the scope of the individual FMEA for the likelihood that the cause and/or failure mode will be detected before the item is released to production.
Risk Priority Number (RPN) and Criticality Number (SO)	Optional tools for evaluating potential risk.

Table 2: SAE J1739 Data Items

The potential *causes* of the *failure mode* are considered and each one is assigned an *occurrence ranking*, 1 to 10. The ranking is relative within the scope of the individual FMEA and is determined without regard to the *severity ranking* or the *detection ranking*. The ranking does take account of

prevention controls; these are means by how a *cause*, *failure mode* or *effect* can be prevented from occurring. The *occurrence ranking* cannot be changed without changing the design such that the *failure mode* is less likely.

The likelihood that a *cause* or a *failure mode* will be detected is assigned a *detection ranking*, 1 to 10. The ranking is relative within the scope of the individual FMEA and is determined without regard to the *severity ranking* or the *occurrence ranking*. The ranking takes into account the *detection controls*, these are means by how a *cause* or a *failure mode* can be detected before the *item* is released to production.

An overall consequence ranking can be arrived at in a number of ways. A classification may be assigned based on the rankings of s*everity*, *severity* and *occurrence*, or *severity* and *detection*. Such classifications can be used to assign *special characteristics* to particular *failure modes* or *causes* to signify that they can have an impact on factors such as safety or compliance to regulations. *Special characteristics* are defined by each organisation. Alternatively, or as well as, the three values may be multiplied together to produce a Risk Priority Number (RPN). This last approach has been criticised by several authors, [173], [174]; the latter on the basis that the scales are ordinal and that an interval scale is required in order for the multiplication operation to be valid.

A fuller exposition of the FMEA technique is given in Appendix B.

2.3.3 Product Safety

Within reliability engineering literature, safety is often quoted as a beneficial outcome, [155], [154], [175], [176]. In mechanical systems, the functionality is constrained by geometry and the continuous nature of the physical properties of materials. The systems tend to have a small number of functions, for which the physics is well-established, and there are only a limited set of modes of operation. For these mechanical systems it has generally been the case that a system that does not fail is also a safe system, e.g. "*If one is examining the hydraulic system of an aircraft, the reliability of that system is more or less complementary to the safety. As reliability increases safety also increases*", [10]. For these mechanical systems the quality techniques, whether based on reliability or robustness, could also be perceived to be sufficient to address the safety issues. But the issues of predicting system values and setting an acceptable target remain.

Mechanical Design

In the context of mechanical engineering, Ullman, [38], discusses three ways to establish product safety. The first way is to design safety directly into the product so that it is inherent. This means that the product poses no inherent danger during normal operation or in case of failure. The second is to design in safety by adding protective devices to the product, e.g. shields, automatic cut-off switches. The third, and weakest, way is the use of warnings, e.g. labels, loud sounds, flashing

lights. In producing a design, he acknowledges that there is uncertainty in the real world due to uncontrollable noises which he lists as unit-to-unit manufacturing variations, aging and environmental conditions. These are addressed by the use of a *factor of safety*, which he also terms a *factor of ignorance*. He defines the *factor of safety* as the ratio of allowable-strength to applied-stress and should have a value greater than 1. There are two ways to estimate the value of an acceptable *factor of safety*: the classical rule-of-thumb method and the probabilistic method of relating it to the desired reliability and to knowledge of the material, loading, and geometric properties. He concedes that the latter is not very precise and the tendency is to use it very conservatively.

For Palh and Beitz, [48], writing in the context of mechanical design, safety is achieved by a combination of the reliable fulfilment of technical functions and the use of protection mechanisms. Safety concerns the operation of the machine, the operator and the effects on the environment. These can be addressed directly using the *safe-life principle* or the *fail-safe principle*, or indirectly. In the *safe-life principle*, based on accurate qualitative and quantitative knowledge, all components and their connections are constructed so that they operate without breakdown throughout their anticipated life. The *fail-safe principle* allows for the failure of a system function, or a component, during service by ensuring that no grave consequences ensue. Redundancy may be used as a means for increasing safety and reliability. Redundancy may be active redundancy, e.g. provision of multiple engines on an airplane, or passive, e.g. standby pumps. Indirect safety is used whenever direct safety methods prove inadequate and is provided by the use of protective systems or protective barriers. These have to operate reliably, function when danger occurs and resist tampering. A protective system should disable the plant, or prevent operation of the plant in a dangerous state, and provide a warning when changes in the working conditions is noted. It may be achieved by the use of redundancy, it may be self-monitoring and it should be testable. During design they also describe the use of a safety factor and use the same definition as Ullman. Cruse, [177], and Bergman *et al*, [178], also describe the use of safety factors in design. Palh and Beitz acknowledge that it is now understood that there is no absolute safety in the sense of complete freedom from danger. Safety measures aim to reduce risks to an acceptable level, but this can only be quantified in a few cases. This can only be determined by technical knowledge, social standards, and the experience of design engineers.

Functional Safety

It was remarked above that, for mechanical systems with a small number of functions and a limited set of modes of operation, it may be legitimate to consider that the safety issues could be addressed by the use of reliability or robustness techniques. In her book *Engineering a Safer World*, [75], Leveson describes this as one of the basic false assumptions that is pervasive in engineering and

other fields. This is certainly the case for software-based electronic control systems where there are typically many modes of operation and the control algorithm is not constrained by physics and geometry. For these types of systems, the role of safety requirements and non-stochastic systematic failures is at least as important as random failures.

To address the perceived need for a new approach for software-based control systems, a new discipline of functional safety has developed in the last thirty years. A number of standards have been published in this time, as mentioned in section 2.2.2. One of significance for this thesis is IEC 61508, [12], which defines functional safety as: "*part of the overall safety that depends on a system or equipment operating correctly in response to its inputs*". The automotive functional safety standard ISO 26262, [13], is an adaptation of this standard, a brief overview was given in section 2.2.2 and a fuller exposition of ISO 2626 is given in Appendix B. Here we note that unlike the automotive FMEA standard, J1739, [159], ISO 26262 does provide a common risk assessment scale for all automotive *E/E systems*. The standard has a prerequisite that the activities necessary to meet its requirements are being carried out under the operation of a quality management. Some of its requirements are effectively enhancing those of a quality management. Its product process requirements are dependent on the *unmitigated risk* assessment performed on the *E/E system* at the vehicle level. It requires that hardware failure rate targets be set for evaluation of the design, and, while providing some possible values, does not mandate particular values. While it acknowledges that some of the safety issues may be addressed by measures, including non-E/E technologies, which are external to the system being developed, their specification and verification are considered to be outside of the scope of the standard. The standard also requires that a *safety case* be produced; this is central to the subject of this thesis.

Levels

The amount of effort and care that does into designing and implementing a system will intuitively be influenced by the consequences of it failing in the field. There are two conflicting considerations; one is a financial concern to not expend more effort than is really necessary and one is a concern to have done everything possible at the time to prevent the failure in the field. To help balance these two conflicting concerns many functional safety and security standards in different domains introduce a categorisation of *levels*. In general, the approach is:

- Perform some assessment to determine how serious the consequences of a failure are;
- Assign a level to the engineering process or one of its artefacts;
- Perform the design and implementation according to requirements dictated by the standard for the assigned level.

Most standards accept that there are two basic causes of failure: random hardware failures and systematic design errors at the system, hardware and software level. Different standards address

one or both. Generally random hardware failures are addressed via probability of failure and systematic errors are addressed through process measures that give assurance or confidence that no unmanaged error remains in the system when it becomes operational, [179].

ARP4754a, [104], defines a Development Assurance Level (DAL), A to E (most rigorous to least rigorous) as the measure of the rigour applied to the development process to limit, to a level acceptable for safety, the likelihood of errors occurring during the process of aircraft/system functions. The Development Assurance Level is assigned depending on the severity classification of the aircraft level failure conditions considering the possible independence between development processes that can limit the consequences of development errors. DALs only addresses systematic faults and not to random faults. DALs can be assigned to functions (FDAL) or to items (IDAL). The significance of a DAL is given by the objectives that it sets. For the systems these are specified in ARP475a, for the software these are specified in DO-178 and for hardware in DO-254.

One of the results of following ISO/IEC 15408, [180], the Common Criteria for Information Technology Security Evaluation for computer security certification, is the assignment of an Evaluation Assurance Level (EAL), which, if met through quality assurance processes, establishes the level of confidence that may be placed in the product's security features. The EAL takes values of EAL1 to EAL7 and as the level increases greater rigour is required for testing and design. The EAL does not specify any hardware failure rates.

IEC 61508, [12], requires that the risks associated with equipment and its electrical/electronic/programmable electronic system should be assessed and compared against a tolerability criteria. If the risk is intolerable, risk reduction measures must be taken. The stringency of the risk reduction measures is assigned a Safety Integrity Level (SIL) which takes values of SIL1 to SIL4, with SIL4 being the most stringent. The value of the SIL sets a limit on the probability of a dangerous failure, either per hour or on demand. The standard requires that safety requirements are derived to prevent or manage dangerous failures, each safety requirement also has an associated value of SIL which is used to indicate which process requirements of the standard are to be met. Meeting these process requirements does not imply values for the probability of failure.

In common with other sector specific standards adapted from IEC 61508, ISO 26262, [13], requires that the *unmitigated risk* associated with the *item* is assessed by identifying *hazardous events* which are assigned an Automotive Safety Integrity Level (ASIL). The ASIL is inherited by all safety requirements derived to prevent or mitigate the *hazardous event*. Again, the ASIL indicates which process requirements of the standard are to be met and, as mentioned above, that hardware failure rate targets be set while not mandating particular values be set or met. A fuller exposition of ISO 2626 is given in Appendix B.

2.3.4 Product Assurance Discussion

In quality engineering the qualitative approach is taking precedence over the quantitative approach with the adoption of processes based on robustness and failure mode avoidance. The FMEA technique is at the centre of all these approaches. Safety in mechanical engineering is based around the use of protective devices and safety factors while, for *E/E systems* development, it is the functional safety approach that dominates E/E. The concept of integrity with regards to the rigour with which systems are developed is common practice, but there is a lot of variation in how this is applied.

2.4 Safety Arguments

As discussed, when a product is placed into operation or the market place, the supplier will wish to claim that it is *safe* according to the definition they use. A claim such as this should be justified, and an argument is the means of justifying the claim. Argumentation formats can be traced back to Stephen Toulmin's work in the 1950s, [181], who produced a general model for reasoning about issues that could not be known with certainty. The Toulmin model has three main components: the claim that is the conclusion of the argument, the support which is provided by evidence for the claim and the warrants which are the accepted belief or value systems that link the evidence to the claim. There are also three supporting components to the model: the backing which justifies that the warrants are appropriate and acceptable, the qualifiers which limit the scope for the claim and rebuttals which consider alternative viewpoints.

This argument framework has been applied to arguments to support safety claims for man-made machines. One approach is the *claims-argument-evidence* model where claims are the same as Toulmin's claims, evidence is the same as Toulmin's grounds and argument is a combination of Toulmin's warrant and backing, [182]. Goal Structuring Notation (GSN), [183], [184], [185], is a graphical notation for documenting a safety argument which is also consistent with the Toulmin model, [182] The automotive functional safety standard ISO 26262, [13], requires a safety case which it defines as: "*an argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development*". An example of an automotive safety argument is given in [186]. Further guidance on how to structure an automotive safety argument is given by MISRA, [187]. This is based on a hierarchy of safety requirements at different levels of abstraction, i.e. safety goals, functional safety requirements, technical safety requirements, hardware safety requirements and software safety requirements. Claims are made at each abstraction level regarding the relationship between the safety requirements at that level and those at the next higher level. Claims are also made at each abstraction level regarding the safety requirements and the corresponding design artefacts. MISRA also propose a categorisation of claim types: claims which concern the technical adequacy of the safety

requirements (*rationale*), claims which concern the relationship between the safety requirements and the corresponding product artefacts (*satisfaction*), claims which concern the processes tools and people used to perform a specific activity (*means*) and claims which concern the nature of the organisation responsible for performing these activities (*organisational environment*). The *rationale* claims have much in common with documenting the design rationale and the need to do this has been long known, [188].

2.4.1 Safety Argument Discussion

The role of the safety case in automotive is increasing due to the ISO 26262 requirement for one to be written. Much of the material already produced as a result of systems engineering, quality and safety activities can be included in a safety argument using the MISRA framework. An argument that covers the entirety of a *mechatronic* system provides a much stronger claim to the system safety than is currently the case as it would allow the reasoning about the non-*E/E technologies* to be included. We adopt the MISRA approach based around a hierarchy of safety requirements at different levels of abstraction.

2.5 Conclusion of Literature Review

One of the objectives of the literature review was to determine if there existed a description of a *mechatronic system* in terms of requirements decomposition through levels of design abstraction which could serve as the basis of a safety argument. While the system engineering principles are relevant there was no model we could build on. Abstraction levels like system, sub-system and component have explanatory usefulness but do not correspond neatly to real world solutions. Therefore, it is necessary to produce our own description to use as the basis for the safety argument. This is addressed in Chapter 3.

The automotive industry has a functional safety standard, ISO 26262, [13],which is a member of the IEC 61508 family of standards and it has been voluntarily adopted by the industry. It provides a good base for the work on an automotive *mechatronic system* safety argument as it is an automotive standard, the risk assessment is independent of implementation and it requires a safety argument. Therefore, we adopt this as our base safety standard. We also adopt the MISRA approach, [187], for structuring the safety argument as it is the most mature work in this area. We note that while the concept of integrity levels is fundamental to the standard it is not part of the mechanical design process; this issue is addressed in Chapter 6.

For the mechanical component evidence necessary to support the mechatronic safety argument we will investigate the use of the FMEA process as this is well established practice within the automotive industry. The feasibility of using it for this purpose is investigated in Chapter 5.

Regarding the topic of risk, we have seen that there is a disconnect between the public perception and the engineering treatment of risk; the engineering community has to follow a technical approach as prescribed by the relevant standards. The assessments of the unmitigated risk, and the sufficiency of risk mitigation, as required by the standards, entail having to make judgements that have a degree of subjectively about them. The engineers making these judgements should have some awareness and understanding of their society's view of risk and be ever mindful that what is assumed to be societally acceptable can, and will, change in the future.

Chapter 3 Design Ontologies and Arguments

3.1 Introduction

The aim of the work is to have a safety argument for a *mechatronic system* that is based systematically on a model of the design. There cannot be a uniform argument if there is no underlying uniform design model; this is the necessary starting point. The unifying design model has to be able to include both the mechanical and E/E the aspects of a *mechatronic system*. We saw from the literature review that such a model does not exist.

We then need to understand how a unifying design model can be used as the basis for the safety argument. As mentioned in Chapter 2, MISRA, [189], has published work on a safety argument framework for an *E/E system*. This is based on the ISO 26262 hierarchy of design levels with associated safety requirements:

- *safety goals* associated with the *item definition*
- *functional safety requirements* placed on the assumed *preliminary architecture*
- *technical safety requirements* placed on the *system design*
- *hardware safety requirements* placed on the *hardware design*
- *software safety requirements* placed on the *software design*

The difficulty of adopting this approach is that there is no commonly accepted equivalent hierarchy of design levels for a *mechatronic system* or a *mechanical system* in the literature and it is not appropriate to speculate about what such a hierarchy might be. The MISRA work published at the time did not cover the *technical safety requirements*, *hardware safety requirements* or *software safety requirements* in any detail, so further work to extend these in this thesis would also not be appropriate. The desire was to base the work on a more basic conceptual model that would be equally applicable to a *mechatronic system*, a *mechanical system* and an *E/E system*. There are no existing safety argument patterns for mechanical components or any argument patterns based on quality processes.

So, there are two challenges: to produce a *unifying design model* and to understand how it can be used as the basis for a safety argument.

In this chapter we propose an approach that could serve as a *unifying design model*. It is a compositional approach based on a generic ontology of design. This generic representation of the design is compared with material in the literature review and issues related to composition are discussed. A generic design process based on the ontology is produced and compared with material in the literature review. We then proceed to understand how the generic ontology of design can be used as the basis for a safety argument and how the compositional aspect of the model is represented

in the safety argument. Finally, we see how well the unifying design model and safety argument fare when applied to an *E/E system*, as understood by ISO 26262.

3.2 Preliminary Considerations

It was decided to approach the modelling task by using ontologies drawn in the SysML Block Diagram notation, [27]. The models produced are similar to Figure 2 and Figure 3 from Chapter 2, which were taken from ISO/IEC 42101, [20], in that they provide both a means of abstracting away from the detail while also providing a degree of formality. The term *ontology* is used in the sense of a formal representation of knowledge by a set of concepts within a domain and the relationships between those concepts, i.e. the type of objects that exist, and their properties and relations, [190].

In this section we produce models of some of the base concepts and subject matter that we need to consider and discuss how different approaches to modelling influence our search for a *unifying design model*.

3.2.1 Flat Ontology Models

It is useful define our understanding of an embedded system by creating a general model which includes both representations of the design and the physical structure, Figure 13. This is based on the literature.

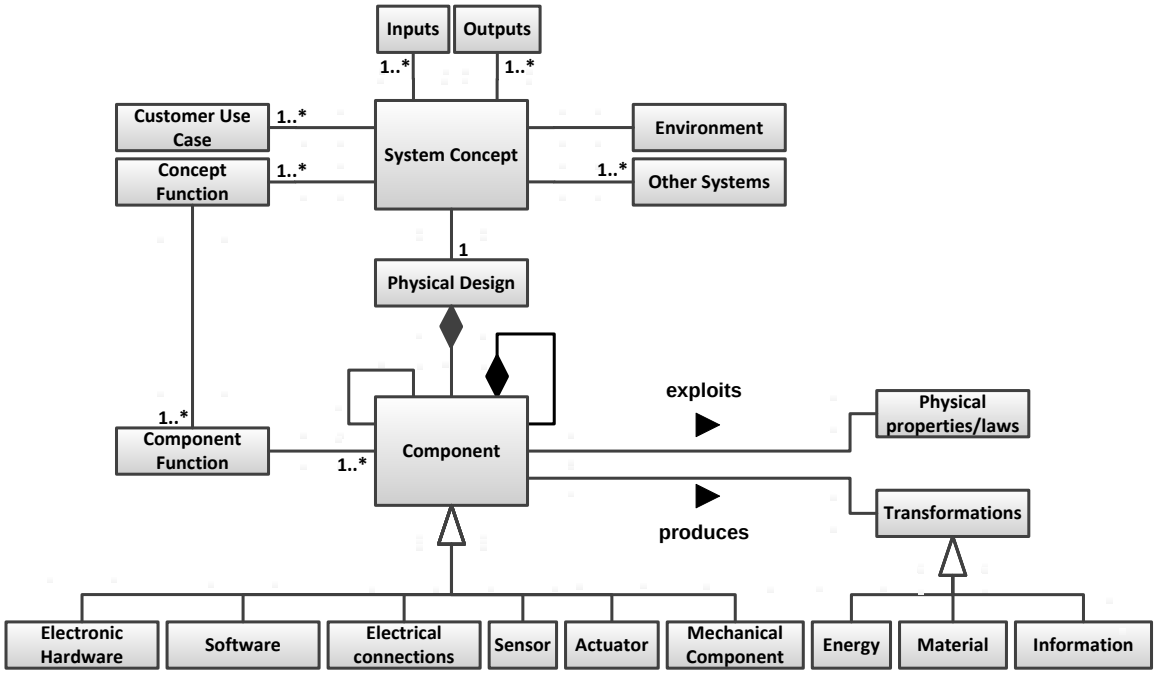

Figure 13: General model of an embedded system

To clarify our understanding of the physical structure of a *mechatronic system* another model was created, Figure 14, although it is accepted that the modelling of the mechanical aspects is superficial.

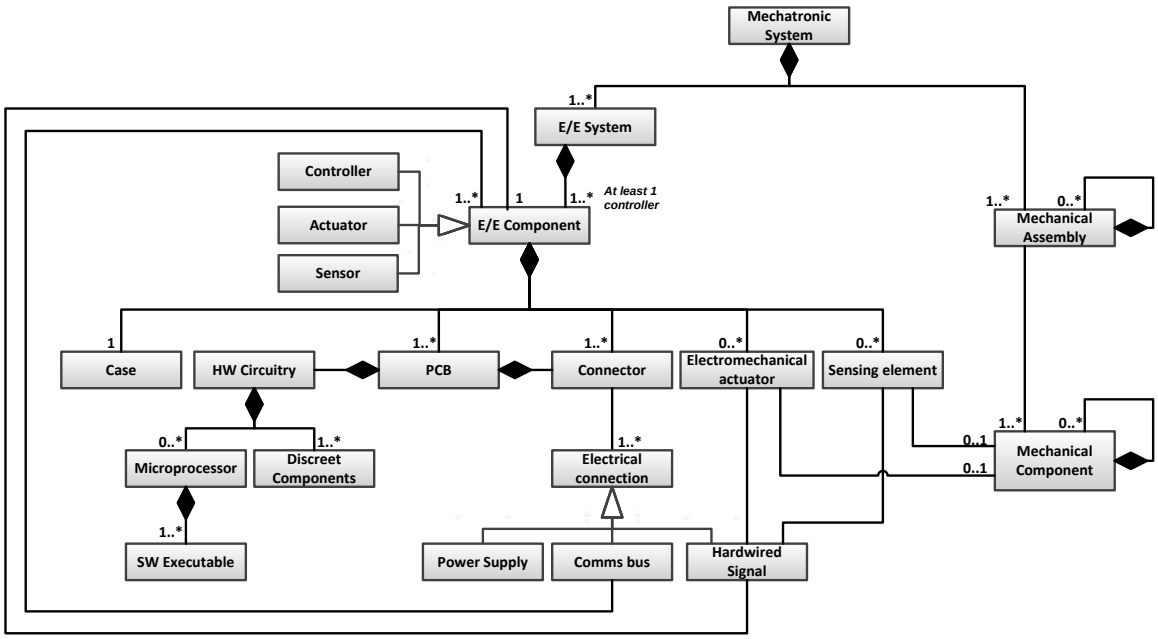

Figure 14: Ontology of the physical structure of a mechatronic system

As ISO 26262 is one our base documents and likely to influence our final model, it is useful to explicitly document its underlying model, Figure 15.

Another key source material is the FMEA. Understanding its relationship to the ISO 26262 model is an important consideration in producing a *unified design model*. Figure 16 shows the models concept, and component FMEAs, taken from Appendix A, are related to our model of ISO 26262.

While providing useful insights into the material we have to handle, these types of models do not form the basis for a unifying model on which a safety argument can be based.

While Figure 13 and Figure 14 use reflexive associations for the physical structure, e.g. a component is constructed from components, the modelling of the design representation does not. For example, in Figure 15 the *functional safety requirements* and *technical safety requirements* appear as separate blocks rather than both being modelled as a single *safety requirements* block. One point taken from this work is that the distinction between a representation of the design and a physical component should be maintained.

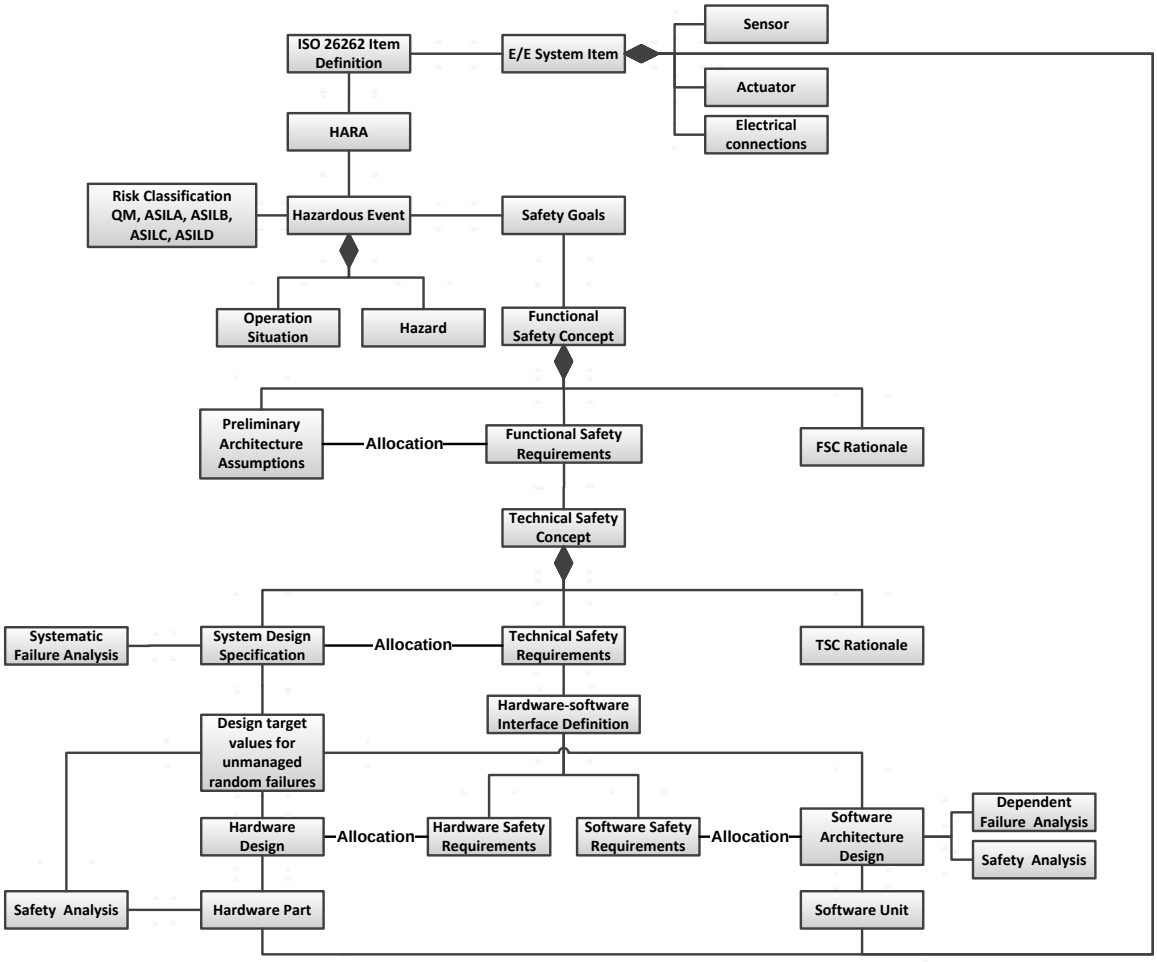

Figure 15: Ontology of ISO 26262

We now proceed to produce a more abstract model of the design process and the physical implementation.

3.2.2 Hierarchical Ontology Model

Taking a more abstract approach, Figure 17 shows a model that is technology-free in that there is no mention of a *mechatronic system* or an *E/E system* and no mention of *hardware design* or *software design*.

A reflexive association is used to show that there is a hierarchy of design representations (*Logical Design*) at different abstraction levels. A reflexive association is used to show that *Physical Parts* may be composed of other *Physical Parts*; the model also shows that one *Physical Part* may also have a non-compositional association with another. The modelling element *Physical Part Description* is used to represent the specification of the *Physical Part*, marking a distinction between the design and the specification for the physical component used to implement the design.

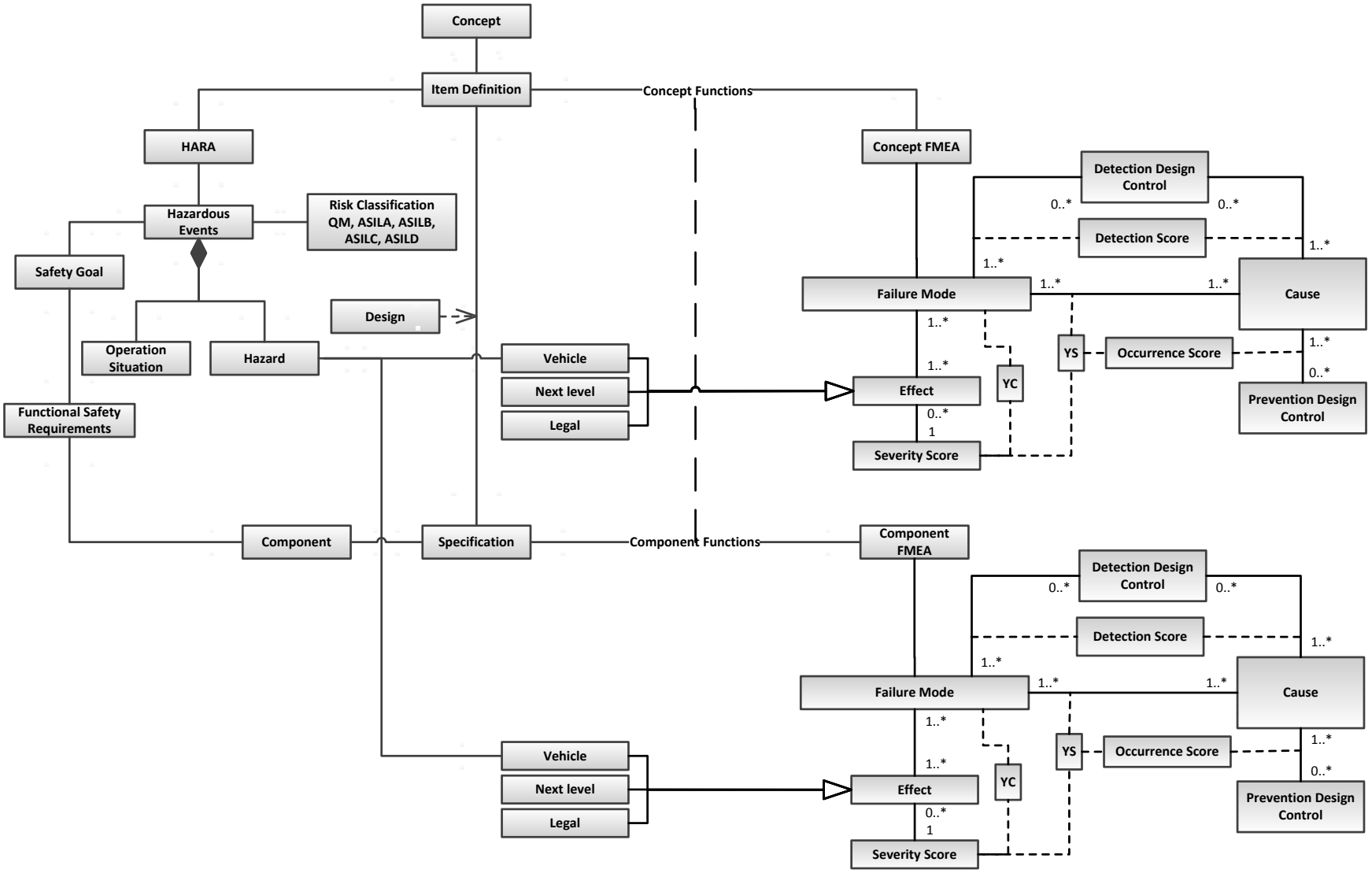

Figure 16: Relationships between HARA and concept and component FMEAs

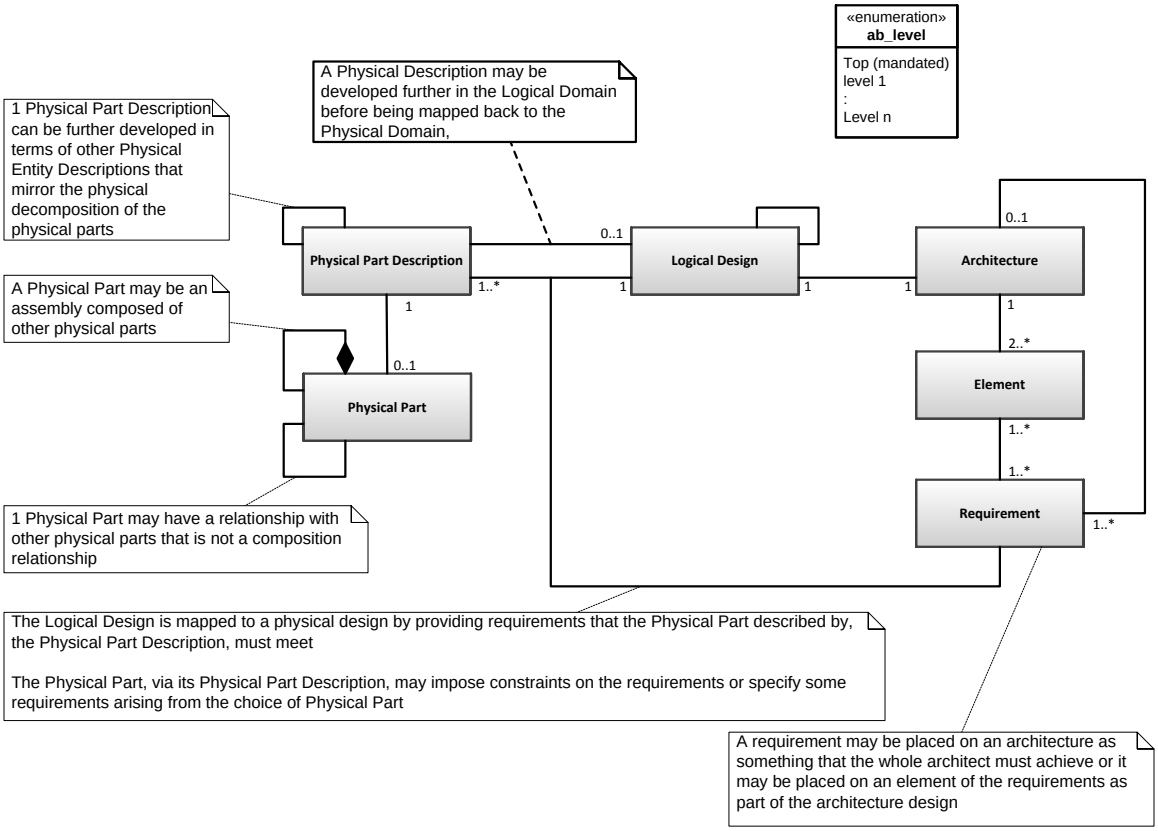

Figure 17: Hierarchical Model

This models the fact that many of the parts will be standard ones that are selected based on the correspondence between their specification and the requirements of the design representation. The *Physical Part Description* can be associated with the design representations at any abstraction level, as standard components can be obtained for many levels of abstraction, for example an assembly of components or a single component. It is also noted that at any level of abstraction there can be both a design representation and a corresponding *Physical Part*. For example, at the *E/E system* level there can be a system design representation and the physical system itself but at a lower level of abstraction there can be the hardware design representation, which is a component of the *E/E system*, and the populated PCB in a case.

While giving these useful insights, a hierarchical ontology model does have some issues. Basing the model on a hierarchy of abstraction levels on the understanding that the design process is one of refining an abstract representation to a concrete one through a set of abstract levels is not always appropriate. For example, when an abstract description of the *mechatronic system* is refined to an abstract description of an *E/E system* and an abstract description of a *mechanical system*, the refinements are both at the same level of abstraction and both proceed separately through further layers of refinement, see Figure 8. Consequently, there is not a view at the same level of abstraction that includes both the *E/E system* and *mechanical system* refinements. The same is also the case

when the abstract description on an *E/E system* is refined to separate electronic hardware and software designs.

3.2.3 Chunked Models

Given the above comments, it is more practical not to use the terminology of levels of abstraction, but rather to think of the design as a set of *chunks*. In this way, some *chunks* can represent an abstraction of other *chunks*, but some *chunks* can also be at the same level of abstraction. *Chunk*s could be defined based on organisational splits, for example between departments or companies, or different technologies, for example mechanical and electronic, because this reflects how products are actually developed. This has the benefit of allowing a division between different engineering disciplines and division between organisations by drawing of boundaries as is appropriate to the situation (these types of boundaries are discussed in the MISRA Guidelines for Safety Analysis [52]). A *chunked* model also allows the refinement of requirements over architecture as it evolves in different *chunks* whose elements consists of different technologies developed by different organisations. Rather than having one model of the whole system representing all levels of abstraction, this allows us to have an ontology model for a single *chunk*. This approach will require a means of defining interfaces between *chunks* to allow one *chunk* to share information with another *chunk* and raises issues of composition. These are addressed in the next section.

3.3 The *Pars* Approach

Rather than continuing to use the term *chunks*, which is seen as being inelegant, it was decided to use the term the *Pars*[1] instead. This term was chosen as the standard engineering terms, such as part and component, already have multiple and context-related definitions

In this section we present the *Pars* approach which consists of an ontology, a process and a design argument pattern. These are all described in the following sections.

3.3.1 Generic *Pars* Design Ontology

The generic *Pars* design ontology is shown in Figure 18.

As has been mentioned, the design process can be seen as an evolution of requirements. The process starts with very abstract representations of requirements and progresses to more concrete requirements. At the same time, the technological solutions start to be introduced, and these proceed from abstract designs to concrete designs realised as specific physical parts. The *Pars* model is intended to be applicable at every stage, but the design representations may take many forms depending on the design or implementation work being performed in the *Pars*.

[1] *Pars* is the Latin for *part* or *component*, *pl Partes*.

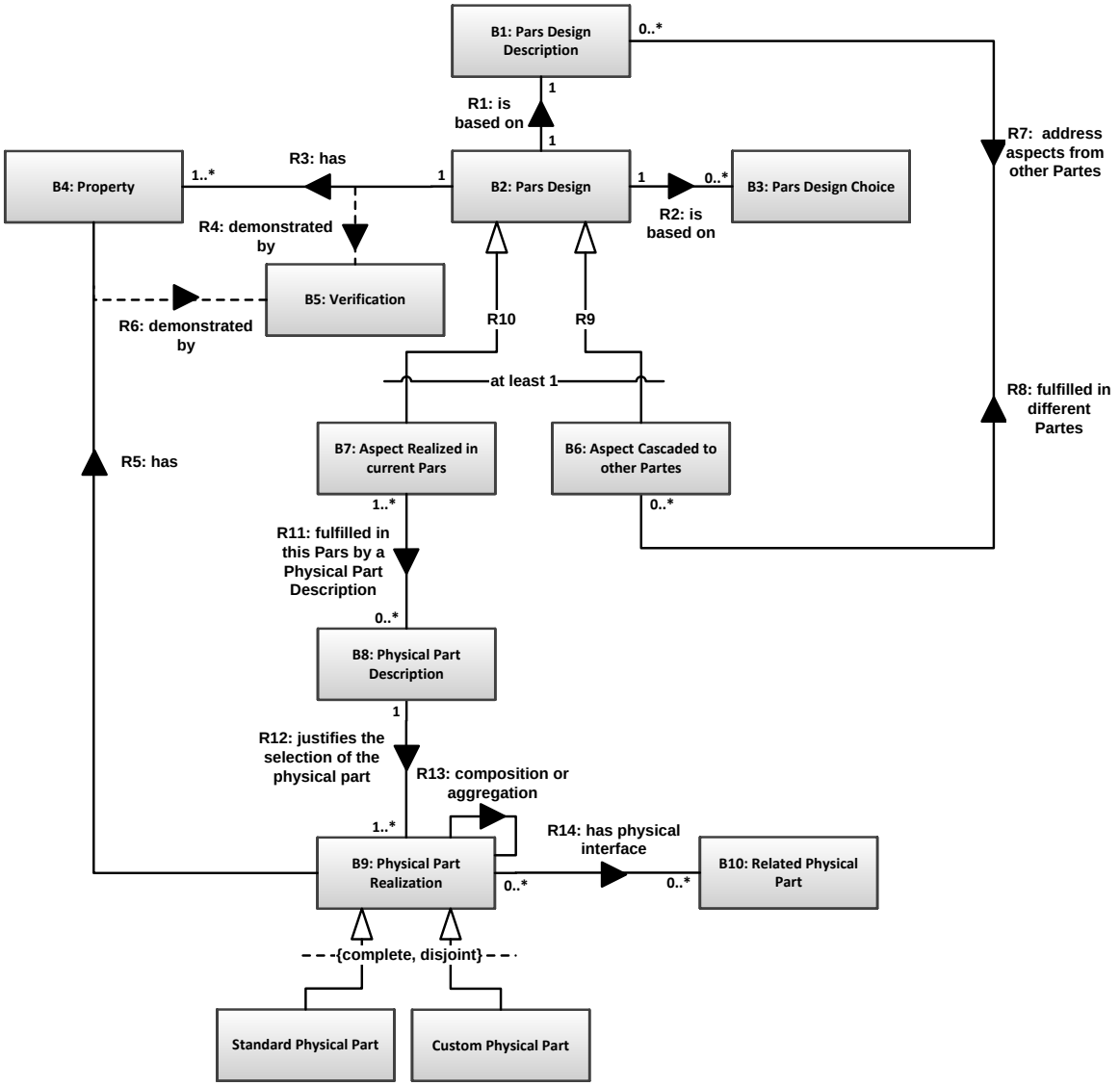

Figure 18: Pars Design Ontology

Design representation may take the form of textual descriptions, requirements, diagrams representing logical structure, e.g. architectures composed of elements, or physical structure. Broy *et al*, [24], acknowledge three categories of representation: informal descriptions, e.g. natural language; formal descriptions, e.g. logical and mathematical expressions with formally defined semantics; and visual representations, e.g. tabular, graphical. The ISO/IEC 42010 conceptual model of an architecture description, Figure 3, can be applied at many levels of abstraction and for different aspects of the design. For instance, there can be a *mechatronic system* architecture description, an *E/E system* architecture, a hardware architecture and a software architecture. Therefore, the definition of the design representation allows for the fact that it may take a variety of forms, Figure 19. In the *Pars* ontology, the blocks B1, B2, B6 and B7 are all design representations.

Except for the first *Pars*, each *Pars* processes one or more *Design Representations* that have been cascaded from other *Pars*. The first *Pars* processes less formal material which is motivating the

work as a whole, for example, evolution of an existing idea or a new inspirational idea. This is discussed further below.

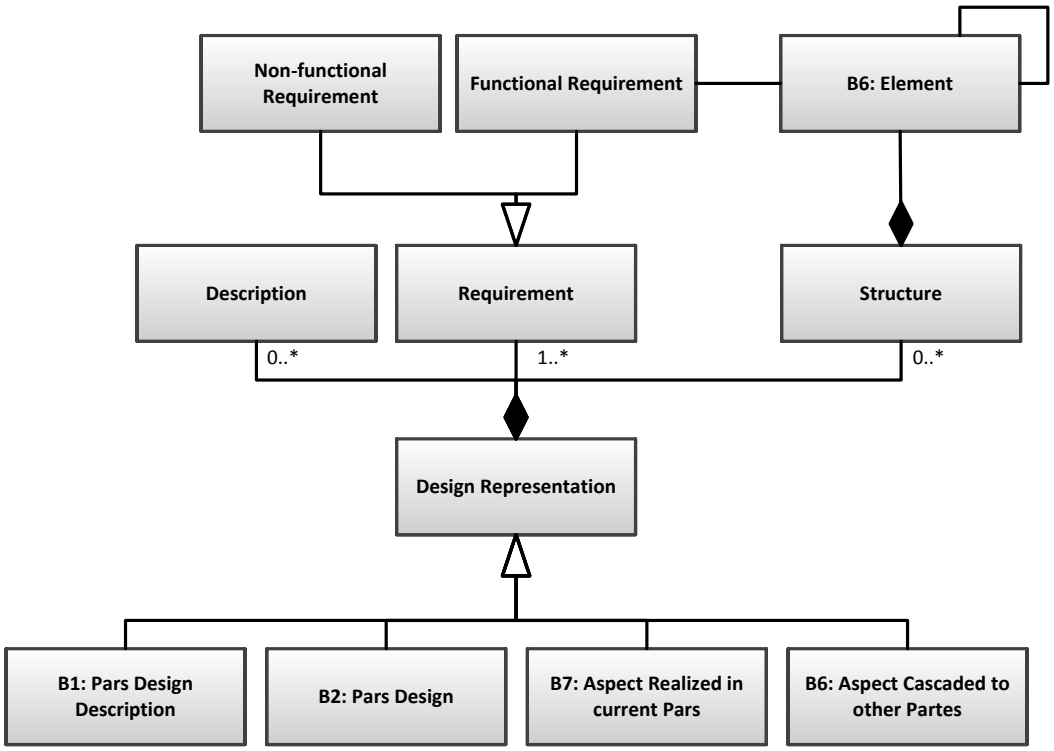

Figure 19: Pars Model - Design Representation

.

Each *Pars* may refine or evolve the design and this may include making choices, block B3, about what standards or regulations are to be met, what design patterns are to be used or what technologies are to be used, Figure 20.

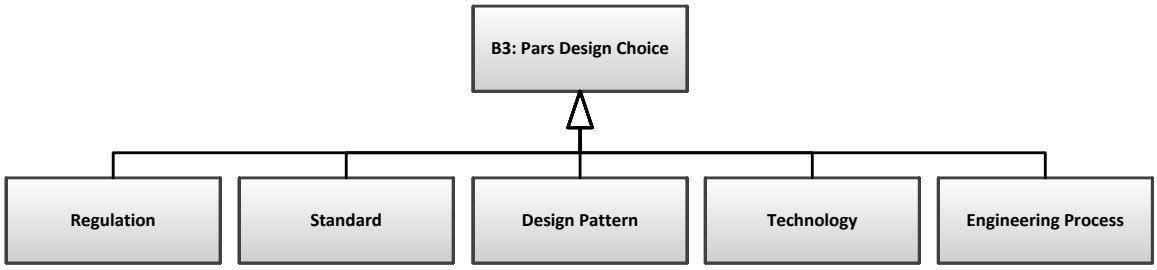

Figure 20: Examples of design choices

The refined or evolved *Design Representation* may be required to exhibit particular properties, block B4. Some properties are part of the *Design Representation* cascaded from other *Partes*, e.g. compliance to functional and non-functional requirements; some properties will arise from the nature of the design or the technology used, e.g. absence of deadlock for a software design. Depending on the nature of the *Design Representation* these may relate to the design material or the anticipated physical realisation of the design, Figure 21.

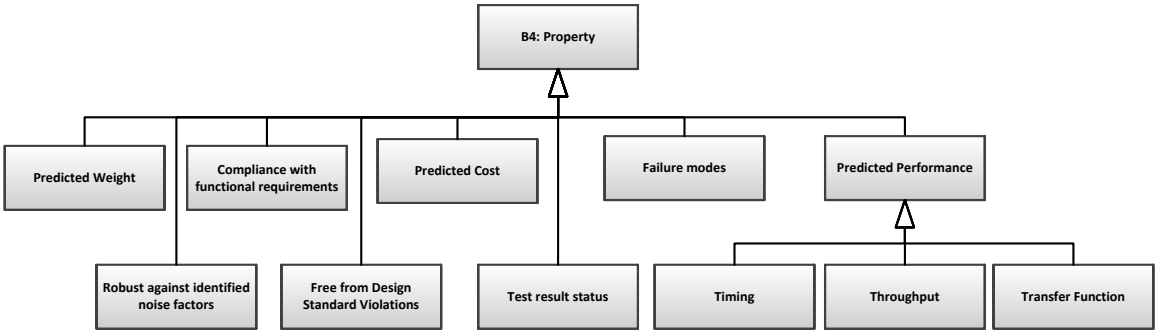

Figure 21: Examples of Property

The presence, or absence, of these properties is established by use of techniques such as inspection, demonstration, test, analysis or simulation, which is represented by block B5. A classification of such techniques by Avizienis *et al*, [191]is given in Table 3. This forms the basis for our model, Figure 22.

Technique	Static	Dynamic
Static Analysis Inspection Review	Y	
Theorem Proving	Y	
Model Checking	Y	
Symbolic Execution		Y
Testing (at multiple levels) Demonstration		Y

Table 3: Verification Approaches (taken from [191])

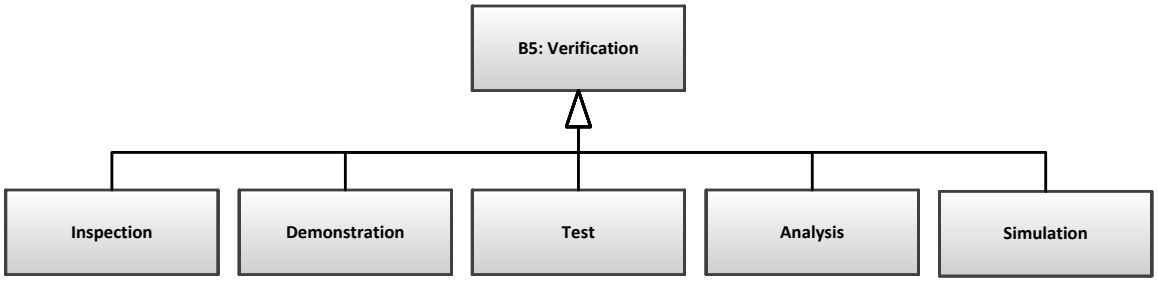

Figure 22: Examples of Verification

Part, or all, of the refined or evolved *Design Representation* may be cascaded to another *Pars*, block B6, or else part, or all of it, may be realised as physical parts, block B7.

Comparison with existing models

In this section we review how this approach relates to the different design models we saw in the literature review, considering the splitting of the overall product development process into *Pars* and the how other ontologies compare with the *Pars* ontology.

The mechatronic V life cycle diagram shown in Figure 8 [46], lists the lifecycle tasks for system, mechanical, electrical and software sub-systems and mechanical, electrical and software components. One possible division of this into a set of *Partes* is a system *Pars*, a system design *Pars*, a mechanical module *Pars*, multiple instances of a mechanical component *Pars*, an electrical

module *Pars*, multiple instances of an electrical component *Pars*, a software module *Pars*, and multiple instances of a software component *Pars*. This is shown graphically in Figure 23, which also shows the interfaces between the *Pars*.

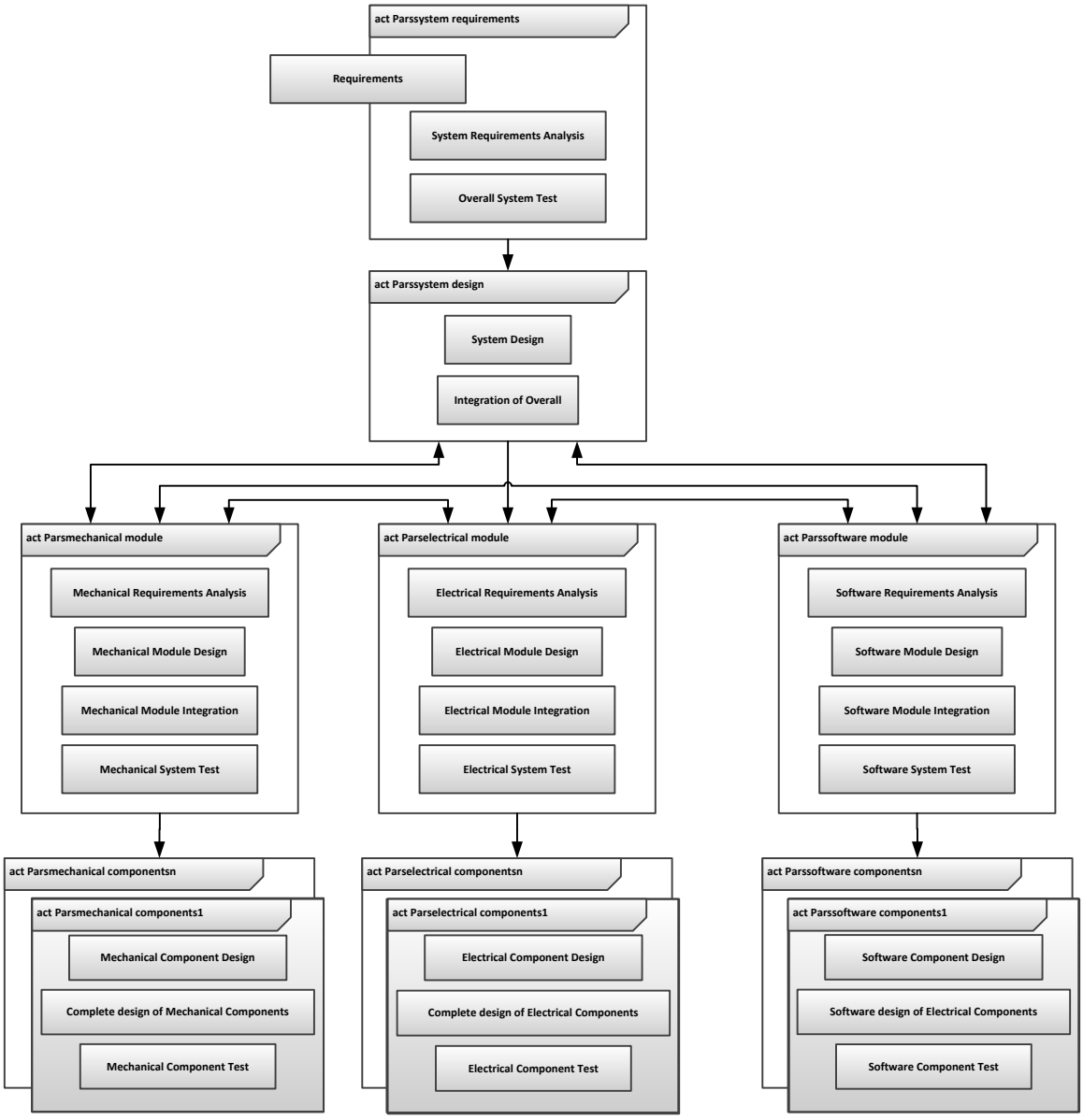

Figure 23: Mechatronic Systems Partes based on [46]

Considering the *Twin Peaks model*, Figure 5 [33], the specification is represented by the *Design Representation*, *B1*, *B2*, *B8* and *B9*; the spiral down occurs as the aspects are cascaded to other *Pars*, *B9*; the solution structure becomes concrete, detailed, as aspects are realized in the current *Pars*, *B8*, *B10* and *B11*; the problem structure evolves in the different *Pars* as they are spawned.

Considering the *Context of architecture description* from [20] Figure 2, an architecture can be part of any *Pars*. For a *mechatronic system* there could be architectures for the *mechatronic system*, the *mechanical system* and the *E/E system*. The elements of the diagram can be related to the *Pars* ontology as shown in the Table 4.

IEC 42010	*Partes*
Stakeholder	Dependent on the *Pars*
System Concern	Design Representation: Requirements
Purpose	Design Representation: Requirements
System	Set of *Partes*
Environment	Design Representation: Requirements
Architecture	Not applicable
Architecture Description	Design Representation: Structure

Table 4: IEC 42010 Architectural Context Blocks vs Partes

The *Pars* model is effectively an *Architectural Viewpoint*; it is written from a requirements perspective, so the stakeholders are those concerned with requirements.

The mechatronic design process shown in Figure 7, [42], could be split into two *Partes*. One, *Pars1*, covering the processes of *Recognition of Need*, *Conceptual Design and Functional Specification*, *First Principle Modular Mathematical Modelling* and *Sensor and Actuator Selection*. The other, *Pars2*, covering the processes of *Detailed Modular Mathematical Modelling*, *Control System Design*, *Design Optimisation*, *Hardware-in-the-loop Simulation* and *Control System Design*. While this split is essentially arbitrary, the rationale is that *Pars1* covers the concept design while *Pars2* covers the detailed design.

When considering the examples of mechanical processes, both the Pahl and Beitz process shown in Figure 9, [48], and the Ullman process shown in Figure 11, [38] can easily be grouped into *Partes*. The mechanical ontologies of these two books are essentially the same with the *Design Representation* variously modelled as *Function Structure*, *Function* and *Sub-functions*, while *Physical Parts*, *B11*, are modelled as *Product*, *Component* and *Assembly*.

Composition Issues

Schemes for decomposing work (requirements, design, etc) are based on the assumption that the separate parts can be brought back together without invalidating any of the required properties of the whole; this capability is referred to as *composability*, [192]. The assumption that the separate parts can be brought back together without invalidating any of the properties of the whole is not necessarily true and to make the assumption when it is not true is called the *Fallacy of Composition*. For the assumption to be true, the resulting behaviour due to the interactions between the parts needs to be completely understood and the requirements for the individual parts defined so as to avoid invalidating properties of the whole. It is one thing to document that this should be the case, it is quite another to achieve it in practice. The problem with a top-down approach being advocated here is that as the system is decomposed into ever more *Pars*, new design decisions are made and specific technological solutions are used. In terms of the design, if we think of a requirement cascaded to another *Pars* as specifying some minimum behaviour, then the requirement is met provided that the behaviour is achieved. But the design produced in the *Pars* may also produce behaviour which exceeds the minimum requirement and which, from the perspective of the

individual *Pars*, is not a problem. But if more than one *Pars* exceeds its requirements in this manner, the result of these behaviours may produce a top-level behaviour which was unanticipated and unwanted. Again, a technology solution will produce behaviours and have properties which were not necessarily part of the specification. The interaction of these with other parts of the system will not have been considered on the top down journey because the choices will not have been made at that time. The *Pars* approach does not solve this problem, it just inherits it as do all schemes that use *composition*.

3.3.2 Generic *Pars* Process

A process has been defined on the basis that it has to produce all the objects of the ontology and establish the relationships between the objects. Figure 24 shows the overall process.

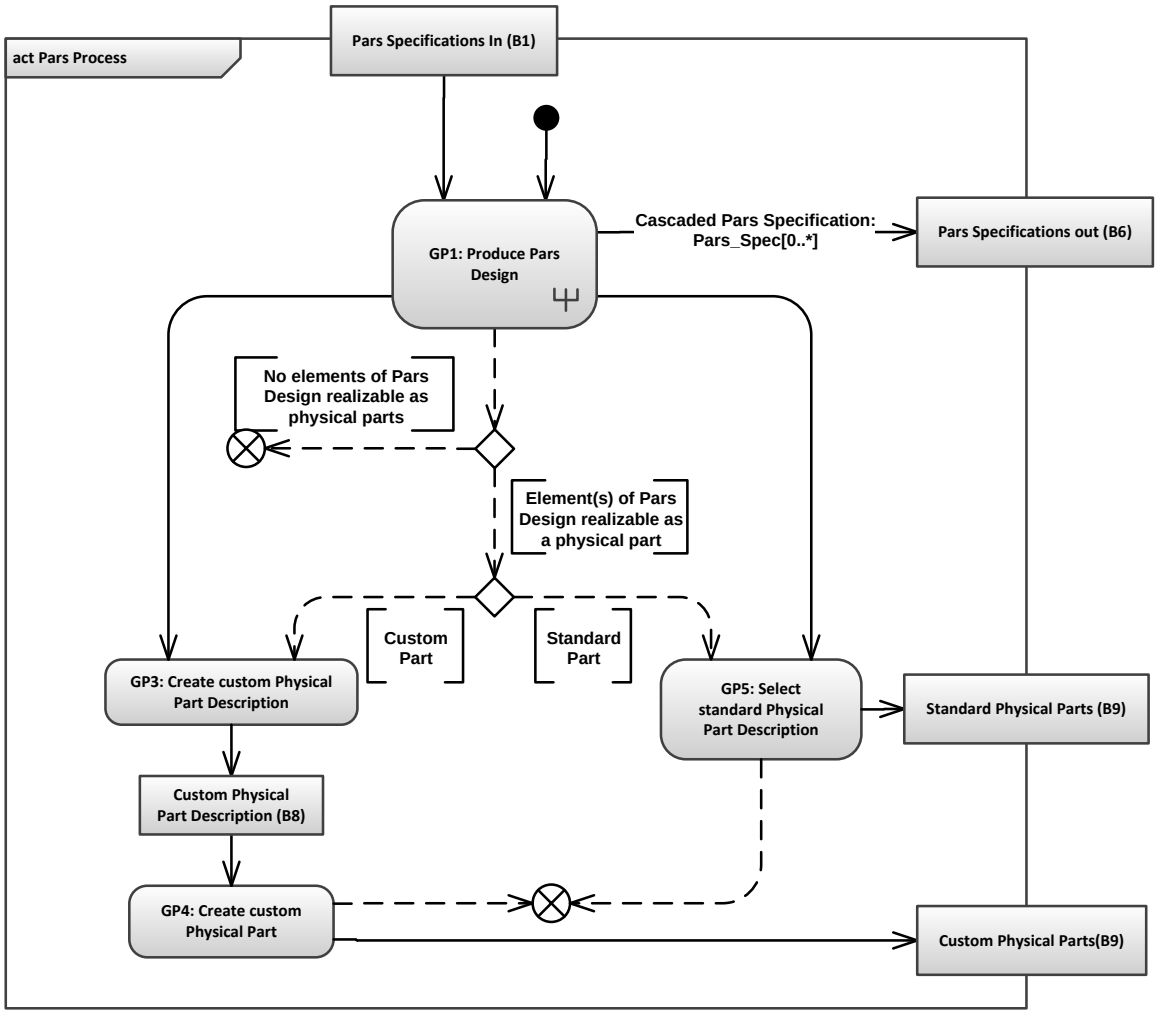

Figure 24: Pars Process

After the initial *Pars*, the input to the *GP1* activity is material cascaded from another *Pars*. The results of the *GP1* activity can be material cascaded to other *Pars* and the creation of physical parts, either standard parts or custom parts. The activity diagram shows both data and control flows. Figure 25 shows the detail for the *GP1* activity.

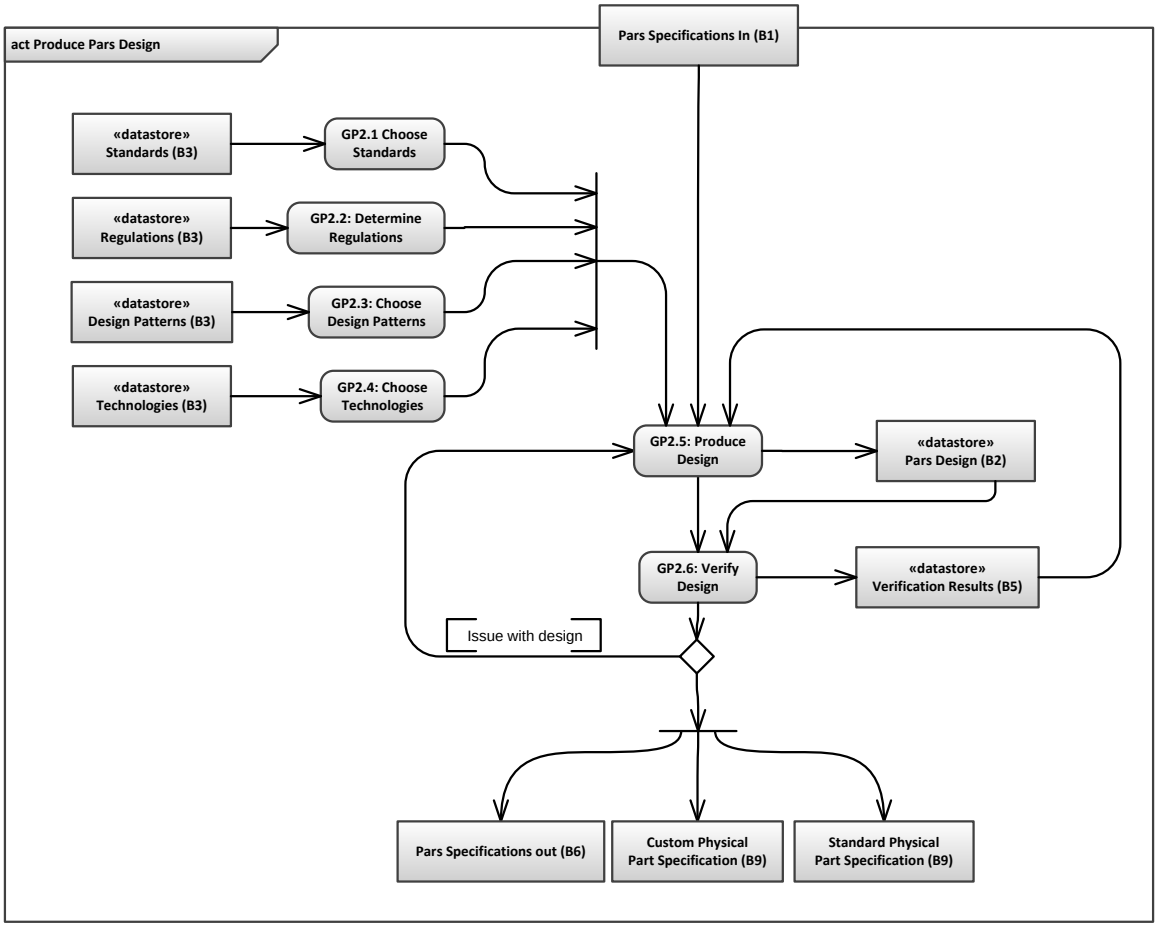

Figure 25: Produce Pars Design Process

The *Pars* choice is shown with the most likely choices that have to be made, i.e. standards, legislation, design patterns and technology. The processing of the input material produces a new design representation with associated required properties the presence, or absence, of which is established through verification.

Comparison with existing processes and literature

In this section we review how the *Pars* process relates to the process examples mentioned in the literature review material. Here we are not considering how the overall product process can be split into *Partes*, but rather the detail within each *Pars*.

Again using the mechatronic design process shown in Figure 7, [42], which we split into *Pars1* and *Pars2* above, the mapping of the mechatronic design processes to the Pars processes is shown in Table 5.

Mechatronic Design Process	***Pars***	***Pars* Process**
Recognition of Need	*Pars1*	
Conceptual Design and Functional Specification		GP2.5 Produce Design GP2.1 - 2.4 Choice
First Principle Modular Mathematical Modelling		GP2.5 Produce Design
Sensor and Actuator Selection		GP2.1 - 2.4 Choice
Detailed Modular Mathematical Modelling	*Pars2*	GP2.5 Produce Design
Control System Design		GP2.5 Produce Design GP2.1 - 2.4 Choice
Design Optimisation		GP2.5 Produce Design
Hardware-in-the-loop Simulation		G2.6 Verify Design
Design Optimisation		GP2.5 Produce Design
Deployment of Embedded Software		Custom Physical Part Specification
Life Cycle Optimisation		

Table 5: Mechatronic Design Processes, [42], mapped to Pars Processes

For the mechanical design process of Ullman, [38], Figure 12, the *Conceptual Design* and *Product Development* both fit with in *GP2.5 Produce Design* and *GP2.6 Verify Design*. The *Document and communicate* of *Product Development* corresponds to the creation of the *Custom Physical Part Specification* and/or the Standard *Physical Part Specification*.

Pahl and Beitz, [48], list the steps of conceptual design and the mapping of these to *Pars* processes is shown in Table 6. The mapping for their steps of embodiment design is shown in Table 7.

Pahl and Beitz Figure 6.1. Steps of conceptual design	***Pars* Process and Documents**
Requirements List	Pars Specification In
Abstract to identify the essential problem	GP2.5 Produce Design GP2.6 Analyse Design
Establish function structures – Overall function, sub-functions	GP2.5 Produce Design (architecture)
Search for working principles	GP2.3 Choose Design Patterns GP2.4 Choose Technologies
Combine working principles into working structures	GP2.5 Produce Design
Select suitable combinations	GP2.5 Produce Design
Firm up into principle solution variants	GP2.5 Produce Design
Evaluate variants against technical and economic criteria	GP2.7 Verify Design
Principle solution (Concept)	Pars Specification out

Table 6: Conceptual Design Steps, [48], mapped to Pars Processes

Pahl and Beitz Figure Figure 7.1 Steps of embodiment design	Pars Process and Documents
Concept	Pars Specification In
Identify embodiment-determing requirements	GP2.6 Analyse Design
Produce scale drawings of spatial constraints	GP2.5 Produce Design
Identify embodiment-determing main function carriers	GP2.6 Analyse Design
Development preliminary layout and form designs for embodiment-determining main	GP2.5 Produce Design
Select suitable preliminary layouts	GP2.5 Produce Design
Develop preliminary layouts and form design for the remaining main function carriers	
Search for solutions to auxiliary functions	GP2.3 Choose Design Patterns
Develop detailed layouts and form designs for the main function carriers ensuring compatibility with the auxiliary function carriers	GP2.5 Produce Design
Develop detailed layouts and form designs for the auxiliary functions carriers and complete the overall layouts	GP2.5 Produce Design
Evaluate against technical and economic criteria	GP2.6 Analyse Design
Preliminary layout	Pars Design
Optimise and complete form designs	GP2.5 Produce Design
Check for errors and disturbing factors	GP2.7 Verify Design
Prepare preliminary parts list and production documents	Pars Specifications out
Definitive layout	Pars Specifications out

Table 7: Embodiment Design Steps, [48], mapped to Pars Process

3.3.3 Generic *Pars* Design Argument

As the *design model* is now based on a division of the work into *Partes*, it follows that the argument also has to be based on a division into *Partes*. As we have defined a *design model* the arguments based on this will also be a *design argument*. We explain in the next section why the same approach can also serve as a safety argument.

Our intention is to base the *design argument* on the *Pars* ontology. A simplistic approach would be to frame claims in terms of the ontological blocks and their inter-relationships, but comparisons with other argument patterns, e.g. MISRA, show that this is not a useful approach. Instead, we chose to approach the problem in a more abstract way by thinking about the structure of the argument for each *Pars* along the lines shown in in Figure 26.

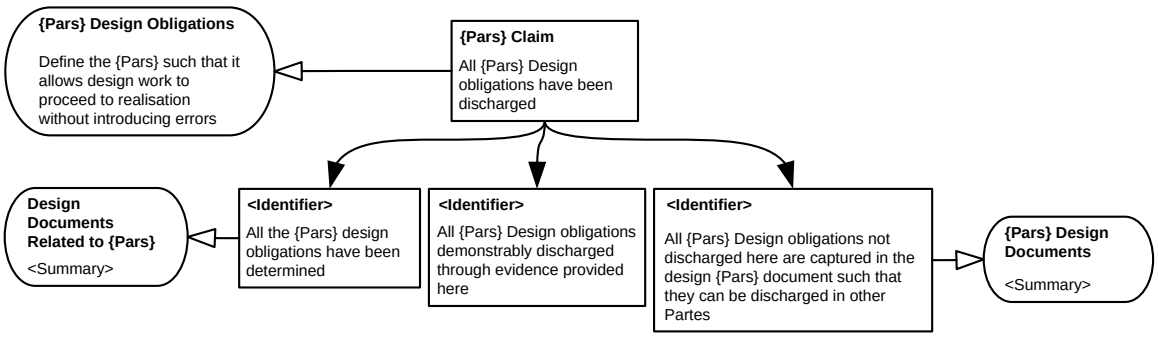

Figure 26: Simplistic Pars Argument

To illustrate how an overall argument may be constructed from an argument split into *Pars*, if a *mechatronic system* was viewed as being designed in the following *Partes*: *mechatronic concept* design, *mechatronic system* design, *mechanical system* design, *E/E system* design, *hardware design* and *software design*, there would be an instance of the ontology and of the argument pattern for

each *Pars*. The argument patterns could link together via *contexts* referencing common design material as indicated in Figure 27.

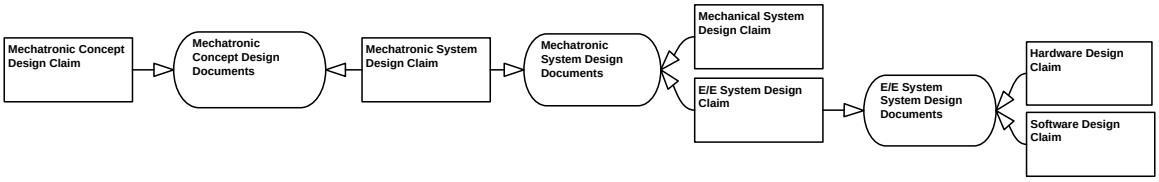

Figure 27: Indicative example of a design argument constructed from Partes

These ideas have been developed and the final pattern, which argues over each design artefact, is shown in Figure 28.

Our approach to producing a pattern for a *Pars* design argument is to base it on the ontology model. The blocks B1 and B2 are generalisations of the *Design Representation* and are instantiated as *design artefacts*. The form these instantiations take will depend on the design process that is being performed in the particular *Pars* and the standards to which the design process is compliant. The block B9 is instantiated as physical realisation artefacts. The form the instantiations take will depend on the nature of the artefact being realised, i.e. hardware, software, mechanical.

Both the *design* and *physical realisation artefacts* have properties that they are required to achieve or display. The properties of the *design artefacts* can be taken from the standards to which the design process is compliant or from what is considered to be best practice as documented in papers and books. For example, in the application of the generic argument pattern to an *E/E system*, we take the properties from ISO 26262. The properties of the *physical realisation artefacts* can be taken from the applicable product standards and will always include compliance with functional requirements.

The argument pattern uses claims that the design and physical realisation artefacts have been produced in accordance with the process and that the properties required of the artefacts have been achieved.

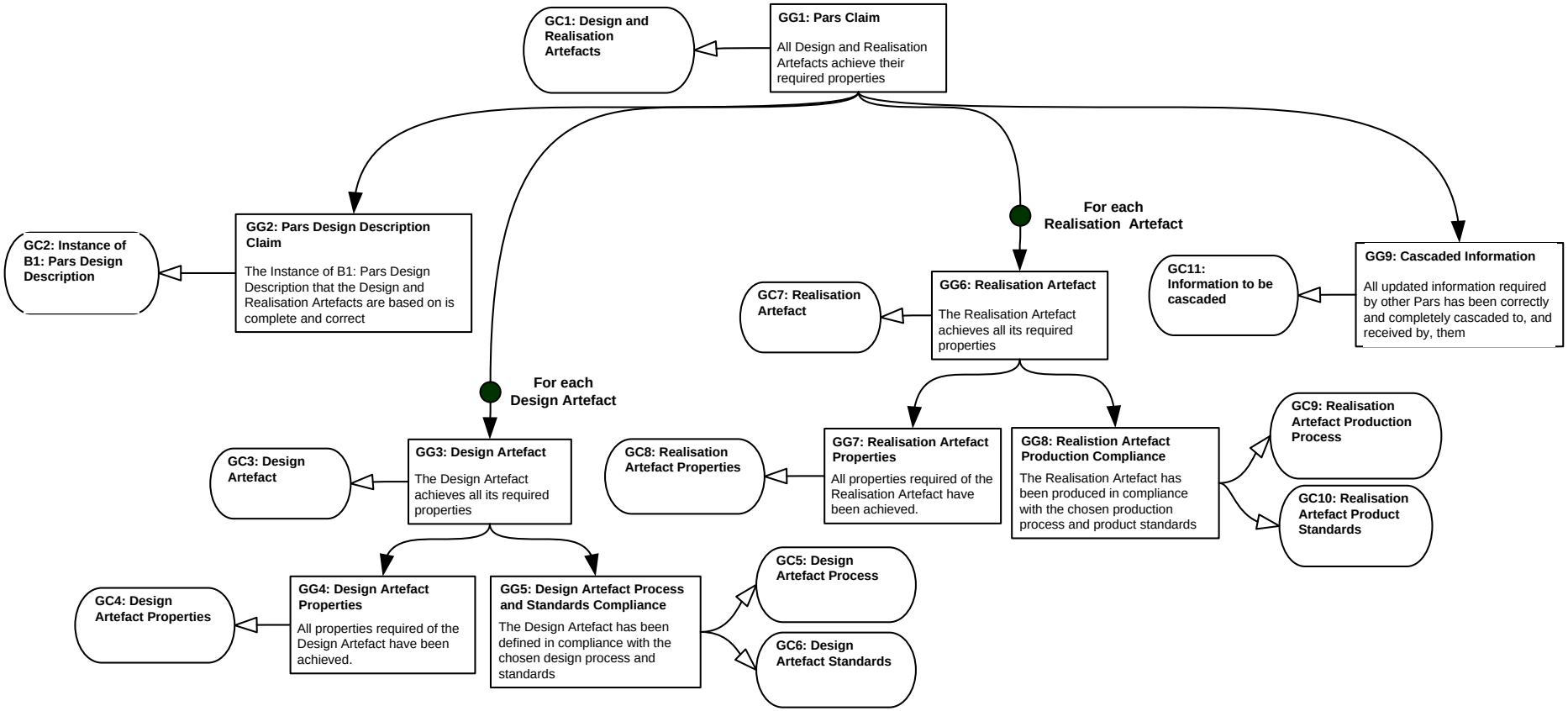

Figure 28: Pars Design Argument Pattern

The argument pattern also uses two claims about the material that is cascaded from one *Pars* to another. One claim concerns the material on which the design and physical realisation artefacts created in the *Pars* are based, represented by *B1: Pars Design Description*. The other claim concerns the material that is cascaded to other *Partes*, represented by *B6: Aspect Cascaded to other Partes*. With the exception of the initial *Pars*, which is discussed in section 3.4.1, the instantiations of *B1: Pars Design Description* consist of material cascaded from other *Partes*. If the same organisation is responsible for one *Pars* and also for the *Pars* that material is cascaded to, then the development of the claim will be based on document control within a single organisation. If the material is cascaded between organisations, then the development of the claim will be based on the correct receipt of up-to-date material.

The generic argument pattern can be described as follows. There is a top claim that all the design and realisation artefacts achieve their required properties. This is developed with the following sub-claims:

- The material that the *design and realisation artefacts* are based on is complete and correct
- Each *design artefact* has been defined in compliance with the chosen design process and standards and has achieved all its properties
- Each *realisation artefact* has been produced in compliance with the chosen production process and standards and has achieved all its properties
- All updated information required by other *Pars* has been correctly and completely cascaded to, and received by, them

3.3.4 Generic *Pars* Safety Argument

A pattern for a design argument was described above; an aspect of the design argument will be a safety argument. This follows because the design argument includes claiming that there is a complete and correct set of requirements and that the corresponding design implements them. The safety argument aspect of this includes claims that there is a complete and correct set of safety requirements which have been correctly implemented. Properties necessary to assure safety are a subset of the general design properties.

A typical top level safety claim is of the form "*The system is acceptably safe to operate*", [185]. The development of this claim typically entails sub-claims concerning:

- The determination of the risk
- The mitigation of the risk such that the system is acceptably safety
- The justification that the risk determination and mitigation have been achieved with sufficient confidence

In the *Pars* approach, risk is a property of the system and it is determined by a hazard analysis and risk assessment process that falls under the scope of *B5: Verification* in the ontology. The definition of acceptable safety will be based on a standard or regulation as part of *B3: Pars Design Choice*. Risk mitigation is achieved through the development and cascading of the design representations, *B1: Pars Design Description*, *B2: Pars Design*, *B6: Aspect Cascaded to other Partes* and *B7: Aspect Realized in current Pars*. Confidence in risk determination and mitigation processes is achieved by compliance with a standard or regulation, chosen as part of *B3: Pars Design Choice*. Compliance is viewed as a property of the design, *B4: Property*, and its assessment process falls under the scope of *B5: Verification*.

3.4 Application to an E/E System

We now apply the generic model described above to the safety argument for an *E/E system*. In the following chapter this will be developed in the safety argument for a *mechatronic system*. We take the description of an *E/E system* from the ISO 26262 standard as it is the safety argument required by this standard that we will extend to a *mechatronic system*. We follow the ISO 26262 standard quite strictly. Figure 29 shows the relationship between the design and safety documentation used by ISO 26262.

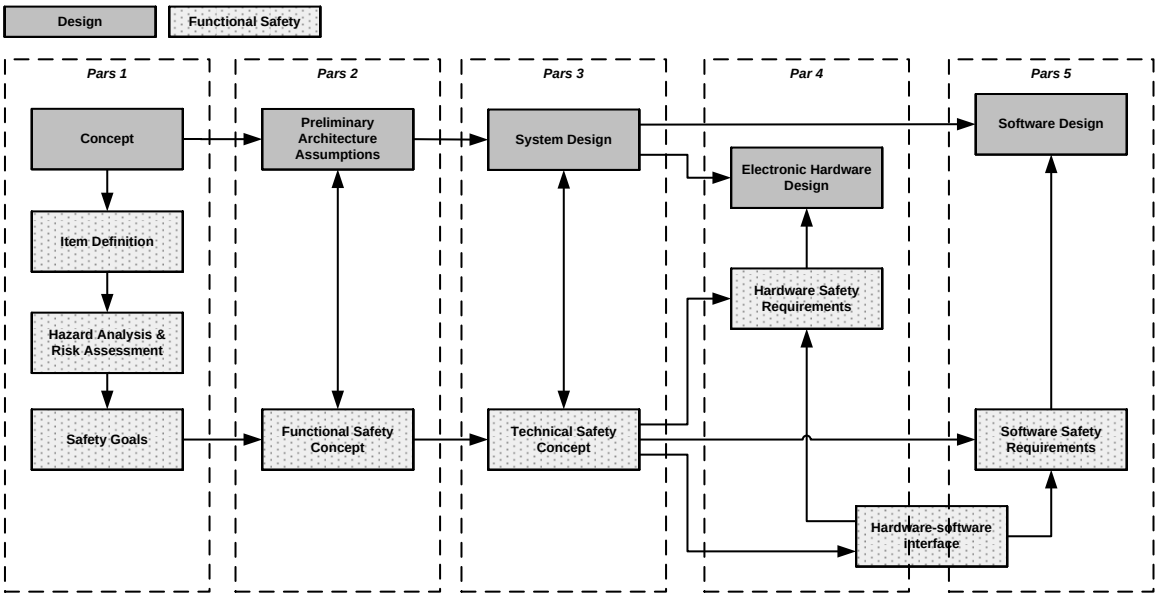

Figure 29: ISO 26262 Design & Safety Documentation

The figure also shows have we have split the documentation into the following *Partes*:

- *Pars 1* Item Definition and the Hazard Analysis and Risk Assessment
- *Pars 2* Functional Safety Concept
- *Pars 3* System Design including the Technical Safety Concept
- *Pars 4* Hardware Design
- *Pars 5* Software Design

In representing the ISO 26262 standard in this way we are trying to add more formality to a document that was not created using a formalism. Our formulisations highlight some issues with the standard. A pragmatic approach has been taken to addressing these. The results of the design process used in the ontology and argument structure do not take account of the sequence in which they are created. Both the ontology and the argument are presented as they are at the completion of all the work. In practice, the design does proceed as a sequence of tasks and the result undergoes changes as the design process iterates around tasks.

A numbering convention is used for the symbols in the ontology diagrams (*PxBy*) and argument diagrams (*PxGy*); *Px* is the number of the *Pars* (*P1 – P5*), *By* is the number of the block from the generic ontology and *Gy* is the identifier for the GSN goal which are numbered sequentially starting with 1 for each individual *Pars*.

3.4.1 Pars 1 Item Definition and the Hazard Analysis and Risk Assessment

The *Pars 1 Item Definition and the Hazard Analysis and Risk Assessment* diagram is shown in Figure 30.

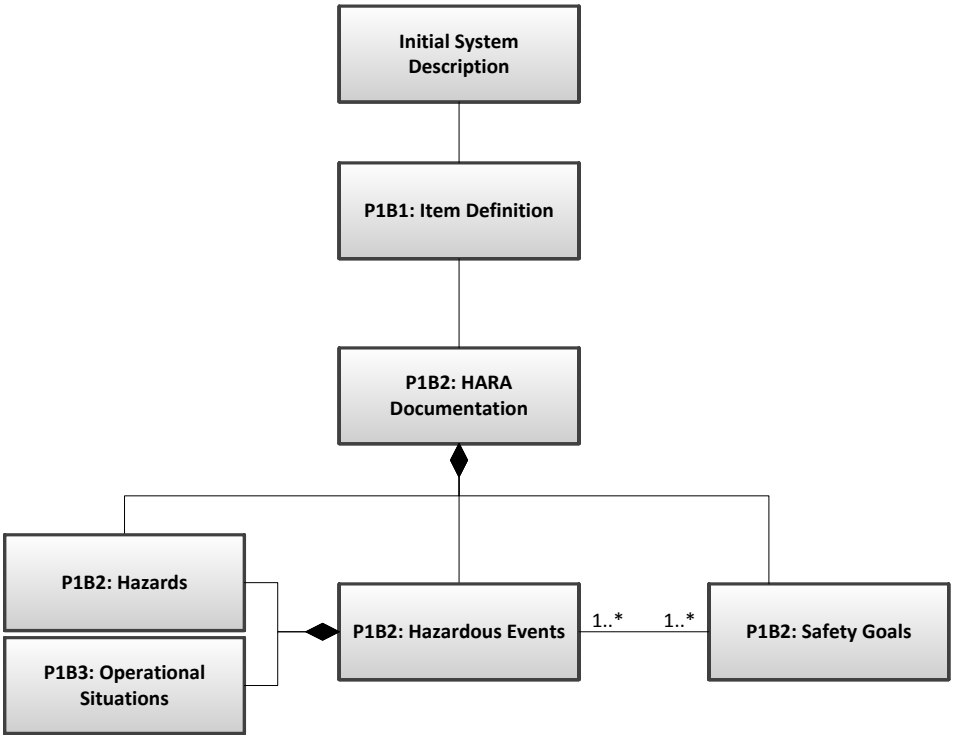

Figure 30: Pars 1 Item Definition and HARA - Pars Design Description and Pars Design

Design

The starting point of a system development is always difficult to model as there is no higher reference point against which it can be verified and as such is outside of any *Pars*. Here we model the primary input to the whole design process as the *Initial System Description*. In ISO 26262 terms in consists of "*product idea, a project sketch, relevant patents, the results of pre-trials, the*

documentation from predecessor items, relevant information on other independent items". We have instantiated the *B1: Pars Design Description* as *P1B1: Item Definition,* but one could argue that it would be equally valid for *PAB1: Item Definition* to be an instantiation of *B2: Pars Design*. The *Item Definition* would document the decision to base the system development on ISO 26262 and this decision is an instance of *B3*: *Pars Design Choice*. The decision is effectively cascaded to the other *Partes* by the assignment of ASIL values to the requirements.

The *B2: Pars Design* is instantiated as *P1B2: HARA Documentation* and it is composed of *P1B2: Hazardous Events* and *P1B2: Safety Goals*. *P1B2: Hazardous Events* is composed of *P1B2: Hazards* and *P1B3: Operational Situations*; the latter is also an instance of *B3: Pars Design Choice*.

It is acknowledged that although hazards are primarily identified in this *Pars*, it is possible for hazards to be identified in *Pars 3 System Design* and *Pars 4 Hardware Design*. This is not explicitly included in the model; any such hazards identified should be communicated to this *Pars* and included in *P1B2: Hazards*. The safety arguments for *Pars 3* and *Pars 4* do acknowledge this but not *Pars 5 Software Design,* as the effects of software errors can only be interpreted as hazards when their effects are understood in terms of the physical interface with the environment.

The *B2: Pars Design* is instantiated as *P1B2: HARA Documentation* and it is composed of the set of documentation required by ISO 26262, namely *P1B2: Hazardous Events* and *P1B2: Safety Goal*s. Each *Hazardous Event* has a value of ASIL assigned to it using the ISO 26262 risk assessment scheme. For the *hazardous event,* the ASIL value indicates the risk associated with it given that no mitigation takes place. Each *hazardous event* has to have one or more *safety goals* associated with it. The s*afety goal* also has an ASIL value assigned to it which corresponds to the highest value of that of its associated h*azardous events*. For the s*afety goal,* the ASIL value indicates the integrity with which safety requirements have to be met.

It is *P1B2: Safety Goals* that is cascaded to the Functional Safety *Pars* and as such represents an instance of *B6: Aspect Cascaded to other Partes*.

Physical Realisation

This *Pars* does not include any physical realisation.

Design Properties

The design properties of *P1B2: Hazardous Events* required by ISO 26262 are that they are:

- compliant with the *Item Definition*
- complete with regard to *Operational Situations* and *Hazards*
- consistent with related *Hazard Analyses* and *Risk Assessments*

- consistent regarding the assignment of ASIL values to *Hazardous Events*

These properties are established by the use of analysis and review techniques given in the standard.

The design properties of *P1B2: Safety Goals* required by ISO 26262 are that they

- completely cover all of the *Hazardous Events*

This property is established by the use of review techniques given in the standard.

Safety Argument

An instantiation of the generic argument for *Pars 1* is shown in Figure 31

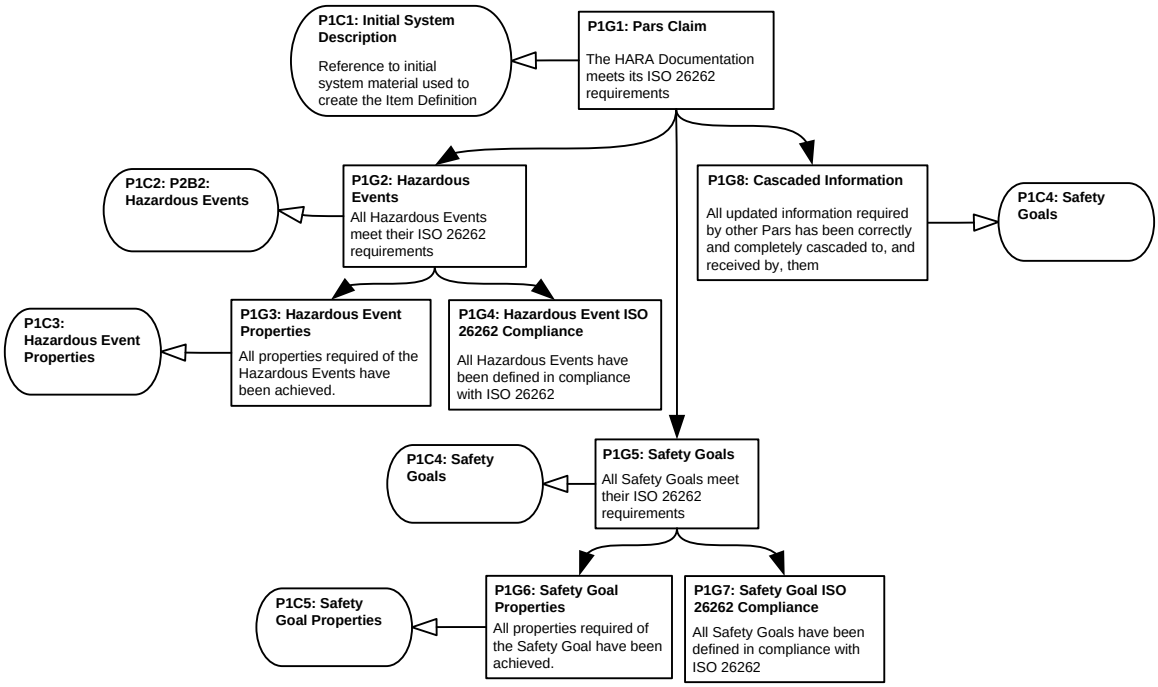

Figure 31: Item Definition and the Hazard Analysis and Risk Assessment Safety Argument

The generic claim *GG2: Pars Design Description* is not instantiated as we take the MISRA approach whereby this claim is argued as part of *P1G4: Hazardous Event ISO 26262 Compliance*; see the discussion below.

The argument is structured around the HARA Documentation; a claim is made for both the *Hazardous Events* and the *Safety Goals* that they meet all their ISO 26262 requirements. Each of these has two sub-claims; one that it has been created in accordance with the requirements of ISO 26262 and the other that it achieves all the properties required by ISO 26262. To substantiate the first of these, further claims and supporting evidence will be based on compliance with the requirements of ISO 26262. In terms of the MISRA framework these are *means* claims.

To substantiate the second of these, further claims and supporting evidence will be based on the use of verification techniques such as review and analysis. The claims will be that the required properties have been demonstrated and that the correct techniques have been used. The former

correspond closely to the MISRA framework *rationale* claims. The latter will again be based on the compliance with the requirements of ISO 26262 and correspond to the MISRA framework *means* claims.

The claim, *P1G8*, relates to cascading information to other *Partes*. To substantiate this, further claims and supporting evidence will be based on how the information has been correctly passed from one organisation to another.

Comparison with MISRA Safety Argument Framework

The MISRA ISO 26262 framework is not based on the *Pars* approach and so it is instructive to see how the two sets of claims align.

As we saw in section 2.4, MISRA categorises claims into the four themes of *rationale*, *satisfaction*, *means* and *environment*. While this categorisation of claim types is not explicit in the *Pars* approach, this categorisation can be applied to the claims in its safety argument.

ISO 26262 does not require that *Item Definition* be correct and complete and therefore there are no claims related to this. As described above, supporting such a claim is difficult as there is no higher authority to appeal to. The MISRA framework addresses this by having a single argument for both the *Item Definition* and the *Hazardous Events*. It has a large argument pattern based on the following key claims:

- Hazard identification has been based on a complete and correct *Item Definition*
- All Hazards associated with information in the *Item Definition* have been identified
- All relevant combinations of *Hazards* and *Operational Situations* have been identified
- All identified *Hazardous Events* have been correctly classified

These claims are supported by a number of *rationale* and *means* claims. For all but the first of the key claims the *rationale* claims correspond to the *P1G3: Hazardous Event Properties* claim and the *means* claims correspond to the *P1G4: Hazardous Event ISO 26262 Compliance* claim.

MISRA has two claims for the *safety goals*:

- Achieving yields the absence of unreasonable risk associated with *Hazardous Events*
- The vehicle behaviour satisfies *safety goals*

The first claim is a *rationale* claim which corresponds to the *P1G6: Safety Goal Properties* claim. It also has associated *means* claims which correspond to *P1G7: Safety Goal ISO 26262 Compliance* claim. The second claim is not included in this *Pars* but is included in the *System Design Pars*.

All of the claims need further development and ultimately evidence. There are many ways in which a claim can be developed; the appropriate way depends on the nature of the system and so it is not useful to develop the generic pattern further. The MISRA approach to this is to have a table of

Typical Topics which list some of the possible ways the argument could be further developed together with the evidence that they should provide. This approach could be applied here.

3.4.2 Pars 2 Functional Safety Concept

The *Pars 2 Functional Safety Concept* diagram is shown in Figure 32

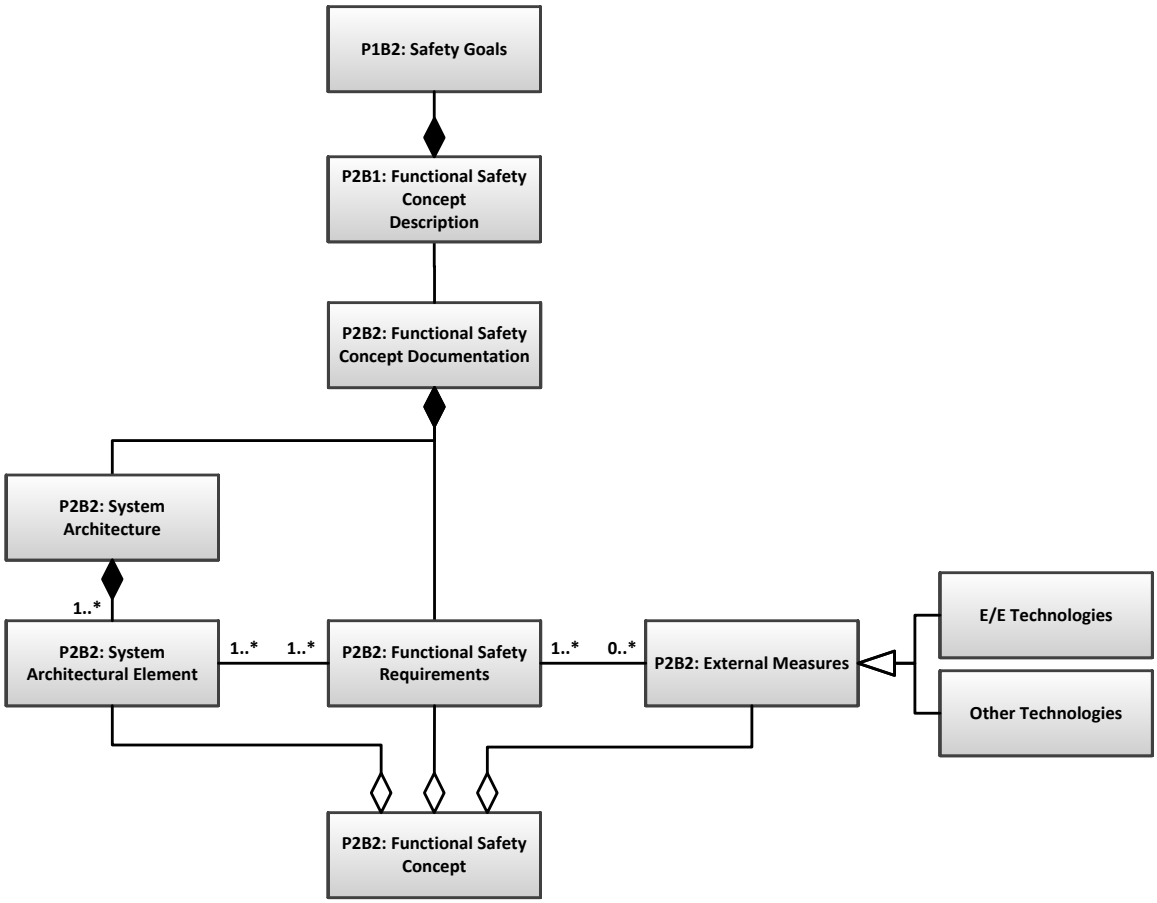

Figure 32: Pars 2 Functional Safety Concept - Pars Design Description and Pars Design

Design

The *B1: Pars Design Description* is instantiated as *P2B1: Functional Safety Concept Description* and it consists of the design material cascaded from *Pars* 1, namely *P1B2: Safety Goals*.

The *B2: Pars Design* is instantiated as *P2B2: Functional Safety Concept Documentation* and it is composed of *P2B2: System Architecture*, *P2B2: System Architectural Element*, *P2B2: Functional Safety Requirements* and *P2B2: External Measures*.

The *Preliminary Architecture Assumptions* of ISO 26262 have been replaced with the *System Architecture, P2B2: System Architecture,* which is seen as being a design choice and so also an instance of *B3: Pars Design Choice*. This approach has been taken as in practice this level of design

has to be kept up to date because it is so central to producing a design that mitigates the assessed risk.

The Functional Safety Requirements, *P2B2: Functional Safety Requirements*, are allocated to elements of the system architecture, *P2B2: System Architectural Element*, and may also be allocated to External Measures, *P2B2: External Measures*. *External Measures* may be other *E/E systems* or non-*E/E systems* and are not considered to be part of the *Item*. Each requirement of the *P2B2 Functional Safety Requirements* will have a value of ASIL associated with it. The source of the value is that of the *Safety Goal* from which it is derived, either directly or as a result of ASIL decomposition. *Functional Safety Requirements* allocated to *External Measures* do not have an associated ASIL value unless the *External Measure* is another *E/E system*.

The *P2B2: Functional Safety Concept Documentation* also includes *P2B2: Functional Safety Concept*. The *Functional Safety Concept* is a work product of ISO 26262, however the definition given in the standard requires some interpretation. The formal definition in part 1 defines it as the "*specification of the functional safety requirements, with associated information, their allocation to architectural elements, and their interaction necessary to achieve the safety goals*". In part 3 the *architectural elements* of the definition are referred as *preliminary architectural elements* of the item and these are an input from an external source which is referred to as *preliminary architectural assumptions*. The Functional Safety Concept could be seen as referring to the *Functional Safety Requirements* and their allocation to both elements of the assumed *Preliminary Architecture* and also to the *External Measures*. The use of the term *concept* implies an idea or rationale and so we take the *Functional Safety Concept* to also include the rationale as to why the functional safety requirements allocated to *E/E system* architectural elements and to the *External Measures* achieve the *Safety Goals*. In doing this, we are picking up on the phrase "*their interaction*" in the formal definition. A similar approach has been taken by MISRA.

It is *P2B2: Functional Safety Concept* that is cascaded to the *System Design Pars* and as such represents an instance of *B6: Aspect Cascaded to other Partes*.

Physical Realisation

This *Pars* does not include any physical realisation.

Design Properties

ISO 26262 only requires design properties of *P2B2: Functional Safety Concept*; these are that it is:

- compliant and consistent with the *Safety Goals*
- is able to mitigate or avoid the *Hazardous Events*
- compliant with the rules of *ASIL decomposition*

These properties are established by the use of analysis and review techniques given in the standard.

Safety Argument

The safety argument for the *System Design Pars* is shown in Figure 33.

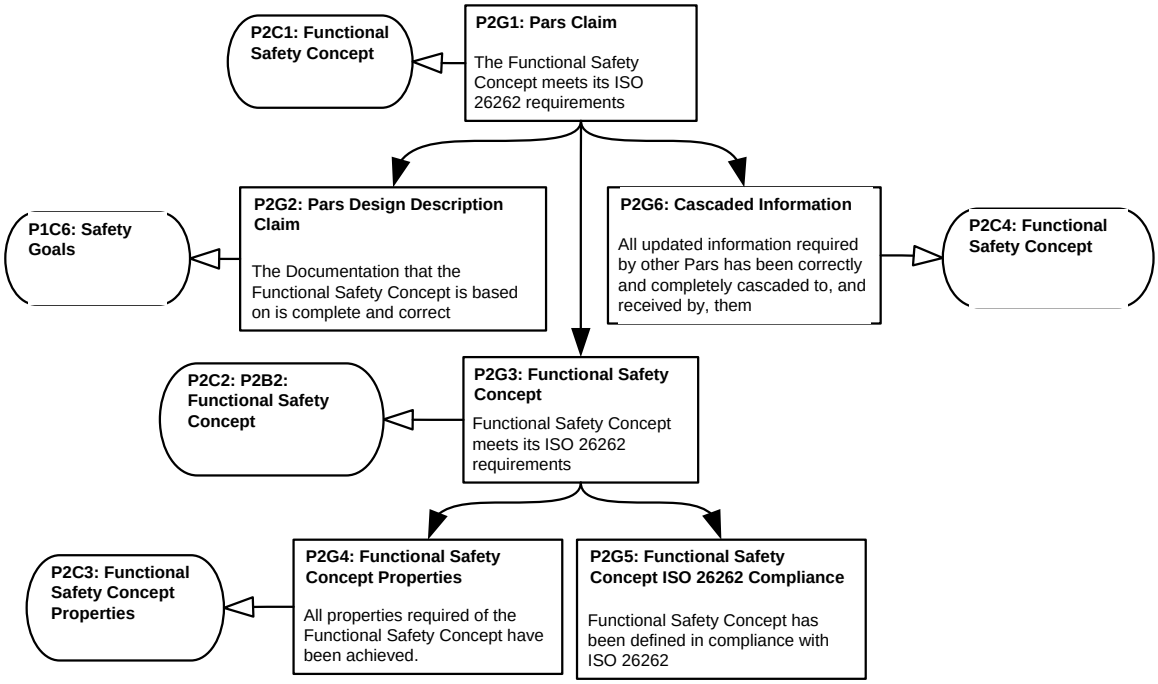

Figure 33: Functional Safety Concept Pars Safety Argument

The argument is structured around the *Functional Safety Concept* for which the claim, *P2G1*, is made that it meets all its ISO 26262 requirements. The *P2G2: Pars Design Description Claim* is a claim made on information cascaded from *Pars 1 Item Definition and the Hazard Analysis and Risk Assessment*. If the *Pars 1* work is conducted by the same team as the *Pars 2* work, then the claim is the same as the *P1G3: Safety Goals* claim. If this is not the case, then the claim is developed by arguing that the information has been correctly passed from one organisation to another.

The *Functional Safety Concept* has two sub-claims; one that it has been created in accordance with the requirements of ISO 26262 and the other that it achieves all the properties required by ISO 26262. To substantiate the first of these, further claims and supporting evidence will be based on compliance with the requirements of ISO 26262. In terms of the MISRA framework these are *means* claims.

To substantiate the second of these, further claims and supporting evidence will be based on the use of verification techniques such as review and analysis. The claims will be that the required properties have been demonstrated and that the correct techniques have been used. The former correspond closely to the MISRA framework *rationale* claims. The latter will again be based on the compliance with the requirements of ISO 26262 and correspond to the MISRA framework *means* claims.

The claim, *P2G6*, relates to cascading information to other *Partes*. To substantiate this, further claims and supporting evidence will be based on how the information has been correctly passed from one organisation to another. This cascading is within this *E/E system*, so the *External Measures*, which are a part of the *Functional Safety Concept*, are not included in the overall safety argument. This is a point that will be picked up in the next chapter.

Comparison with MISRA Safety Argument Framework

MISRA has two claims for the *Functional Safety Requirements*:

- Satisfying the *Functional Safety Requirements* yields the achievement of *Safety Goals*
- The vehicle behaviour satisfies *Functional Safety Requirements*

The first claim is a *rationale* claim which effectively corresponds to the *P2G4: Functional Safety Concept Properties* claim. It also has associated *means* claims which correspond to *P2G5: Functional Safety Concept ISO 26262 Compliance* claim. The second claim is not included in this *Pars* but is included in the *System Design Pars*.

3.4.3 Pars 3 System Design including the Technical Safety Concept

The *Pars Software Design* diagram is shown in Figure 34.

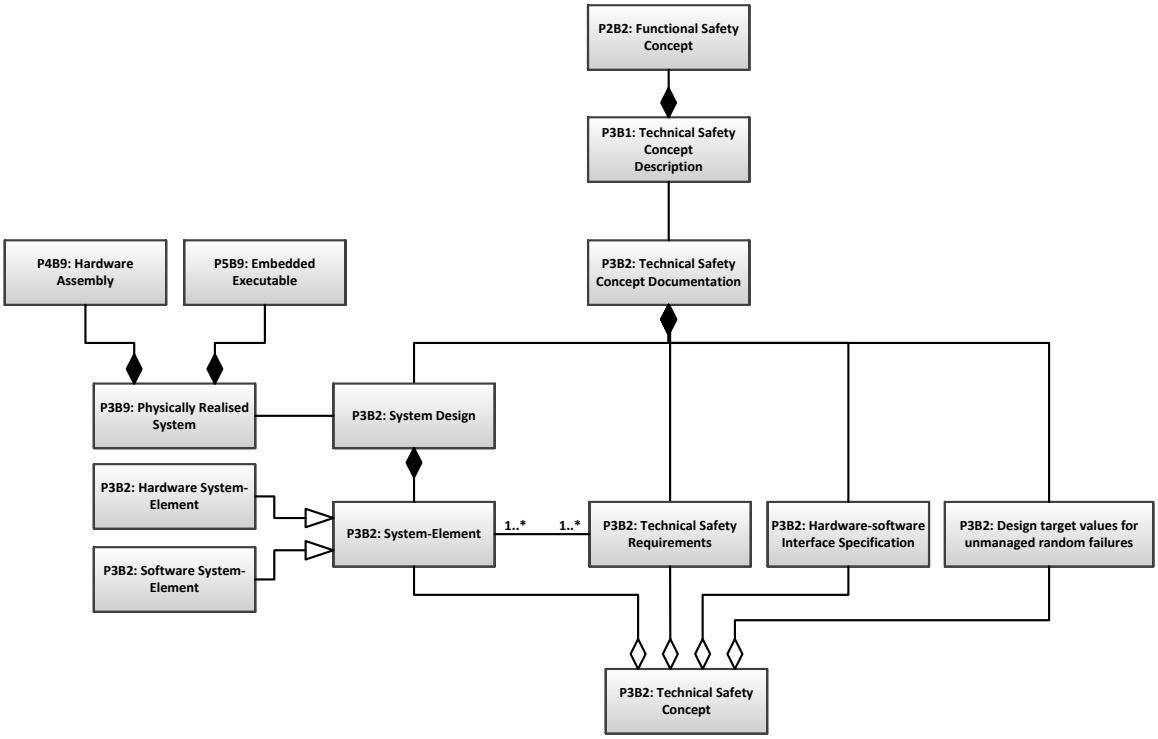

Figure 34: Pars 3 Technical Safety Concept - Design Description, Design & Realisation

Design

The *B1: Pars Design Description* is instantiated as *P3B1: Technical Safety Concept Description* and consists of *P2B2: Functional Safety Concept* cascaded from *Pars* 2. The *Functional Safety*

Concept is composed of the system architecture, the *Functional Safety Requirements* assigned to elements of the architecture, the *External Measures* and the rationale underpinning the safety concept.

The *B2: Pars Design* is instantiated as *P3B2: Technical Safety Concept Documentation* and it is composed of *P3B2: System Design*, *P3B2: System-Element*, *P3B2: Technical Safety Requirements*, *P3B2: Hardware-software Interface Specification* and *P3B2: Design target values for unmanaged random failures*.

The Technical Safety Requirements, *P3B2: Technical Safety Requirements*, are allocated to elements of the system design, *P3B2: System-Element*. The system design is a design choice and so also an instance of *B3*: *Pars Design Choice*. The system elements may be either hardware elements or software elements and interface between the two different types of element is documented in the interface specification, *P3B2: Hardware-software Interface Specification*.

The interface specification documents the interaction between the software and the electronic hardware that executes it and between the software and the services provided by the hardware. The microprocessor executing the software has be configured to operate according to the system design, and the configuration is set up by the software on start-up, typically by writing values into microprocessor registers. Examples of microprocessor facilities to be configured include ports (as inputs or outputs), memory management, communication channels, timers, analogue-digital & digital-analogue converters, interrupts and watchdogs. Other programmable devices may also need to be configured in a similar manner. Where the software uses digital representations of analogue values in the environment, the mapping between the environment value and its representation is defined for both inputs and outputs. The meaning of digital and analogue inputs is defined, for example those that indicate the presence of faults e.g. detection of over-current, short-circuit or over-temperature. The response to these conditions will be specified as *Technical Safety Requirements* cascaded to the software *Pars*. Similarly, where values are communicated over a network the meaning of the digital value is defined.

The hardware elements also have a requirement (for those implementing safety requirements assigned ASIL C or ASILD values) for the design to meet a failure rate target for unmanaged random failures: *P3B2: Design target values for unmanaged random failures*. This target failure rate is a design choice and also an instance of *B3: Pars Design Choice*.

The *P3B2: Technical Safety Concept Documentation* also includes *P3B2: Technical Safety Concept*. Like the *Functional Safety Concept*, the *Technical Safety Concept* is also a work product of ISO 26262, and again the definition given in the standard requires some interpretation. The formal definition in part 1 defines it as the "*specification of the technical safety requirements and their allocation to system elements for implementation by the system design*". Here we have

modelled it in a similar manner to the *Functional Safety Concept* of *Pars 2*, i.e. as embodying the *Technical Safety Requirements*, their allocation and the design rationale. It is *P3B2: Technical Safety Concept* that is cascaded to the *Hardware Design* and *Software Design Partes* and as such represents an instance of *B6: Aspect Cascaded to other Partes*.

Physical Realisation

The *System Design* is implemented by hardware and software elements realised in the *Hardware Design Pars* and the *Software Design Pars*. The realised *System Design* is represented by *P3B9: Physically Realised System* and is composed of *P4B9: Hardware Assembly* and *P5B9: Embedded Executable* from the *Hardware Design Pars* and the *Software Design Pars* respectively.

Design Properties

The design properties of *P3B2: Technical Safety Requirements* required by ISO 26262 are that they are:

- compliant and consistent with the *Functional Safety Concept*
- compliant with the *System Design*
- compliant with the rules of *ASIL decomposition*

These properties are established by the use of review techniques listed in the standard.

The design properties of *P3B2: System Design* required by ISO 26262 are that it is:

- compliant and complete with regard to the *Technical Safety Concept*
- robust against the causes of systematic failures and the effects of systematic faults

These properties are established by the use of review, simulation, and analysis techniques listed in the standard.

Physical Realisation Properties

The properties of *P3B9: Physically Realised System* required by ISO 26262 is that it is:

- compliant with *Hardware-software Interface specification*
- correctly implements the *Functional and Technical Safety Requirements* when operating in the context of the electrical architecture with other controllers
- correctly implements the *Functional and Technical Safety Requirements* and achieves the *Safety Goals* when operating as an *Item* in a vehicle in the context of the electrical architecture with other controllers

Achievement of the *Safety Goals* at the vehicle level includes an assessment of:

- the controllability risk parameter under failure conditions when the system is fulfilling the *Functional and Technical Safety Requirements*
- the effectiveness of safety measures for controlling random and systematic failures
- the effectiveness of the external measures

- the effectiveness of the elements of other technologies

These properties are established by the use of test techniques listed in the standard.

Safety Argument

The safety argument for the *System Design Pars* is shown in Figure 35.

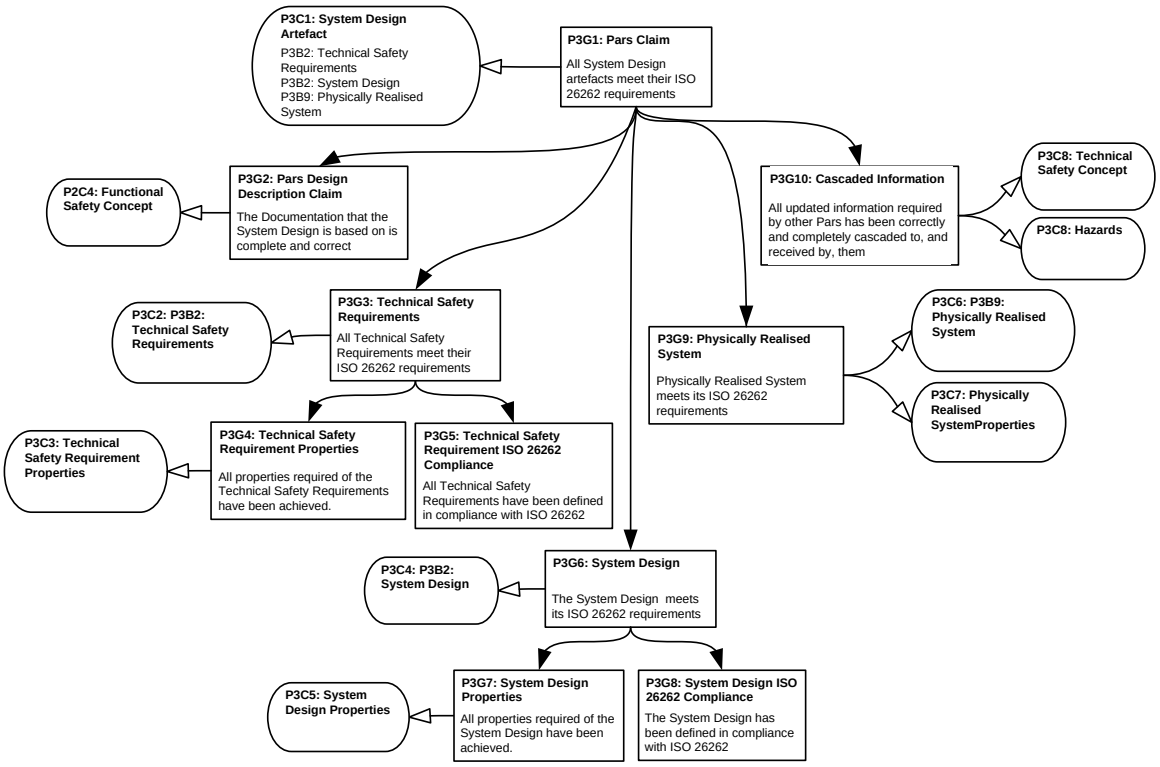

Figure 35: System Design Pars Safety Argument

The argument is structured around the *System Design* artefacts for which the claim, *P3G1*, is made that these meet all their ISO 26262 requirements. The *P3G2: Pars Design Description Claim* is a claim made on information cascaded from *Pars 2 Functional Safety Concept*. If the *Pars 2* work is conducted by the same team as the *Pars 3* work, then the claim is the same as the *P2G3: Functional Safety Requirements* claim. If this is not the case, then the claim is developed by arguing that the information has been correctly passed from one organisation to another.

Each design artefact-related claim has two sub-claims, one that the design artefact has been created in accordance with the requirements of ISO 26262 and the other that the design artefact achieves all the properties required by ISO 26262. To substantiate the first of these, further claims and supporting evidence will be based on compliance with the requirements of ISO 26262 for the appropriate ASIL value, including the correct use of ASIL decomposition. In terms of the MISRA framework these are *means* claims.

To substantiate the second of these, further claims and supporting evidence will be based on the use of verification techniques such as review and analysis. The claims will be that the required

properties have been demonstrated and that the correct techniques have been used. The former correspond closely to the MISRA framework *rationale* claims. The latter will again be based on the compliance with the requirements of ISO 26262 for the appropriate ASIL value and correspond to the MISRA framework *means* claims.

The claim related to the realisation is *P3G9: Physically Realised System*. To substantiate this, further claims and supporting evidence will be based on the use of test techniques. The claims will be that the required properties have been demonstrated and that the correct techniques have been used. The former correspond closely to the MISRA framework *satisfaction* claims because they concern the relationship between the safety requirements and the corresponding product artefacts. The latter will again be based on the compliance with the requirements of ISO 26262 for the appropriate ASIL value and correspond to the MISRA framework *means* claims.

The final claim, *P3G10*, relates to cascading information to other *Partes*. To substantiate this, further claims and supporting evidence will be based on how the information has been correctly passed from one organisation to another.

The MISRA framework published for public review did not cover this or any of the remaining *Pars* in any detail so a comparison is not possible.

3.4.4 *Pars 4*: Hardware Design

The *Pars Hardware Design* diagram is shown in Figure 36.

Design

The *B1: Pars Design Description* is instantiated as *P4B1: Hardware Design Description* and it consists of *P3B2: Technical Safety Concept* cascaded from *Pars* 3. The Technical Safety Concept is composed of the system design, the Technical Safety Requirements assigned to elements of the system design, the *Hardware-software Interface* specification, the design target values for unmanaged random failures and the rationale underpinning the safety concept.

The *B2: Pars Design* is instantiated as *P4B2: Hardware Design Documentation* and it is composed of *P4B2: Hardware Safety Requirements* which are allocated to *P4B2: Hardware Design*. ISO 26262 describes the hardware design as being composed of both an architecture, *P4B2: Hardware Architecture*, and a detailed design, *P4B2: Hardware Detailed Design*.

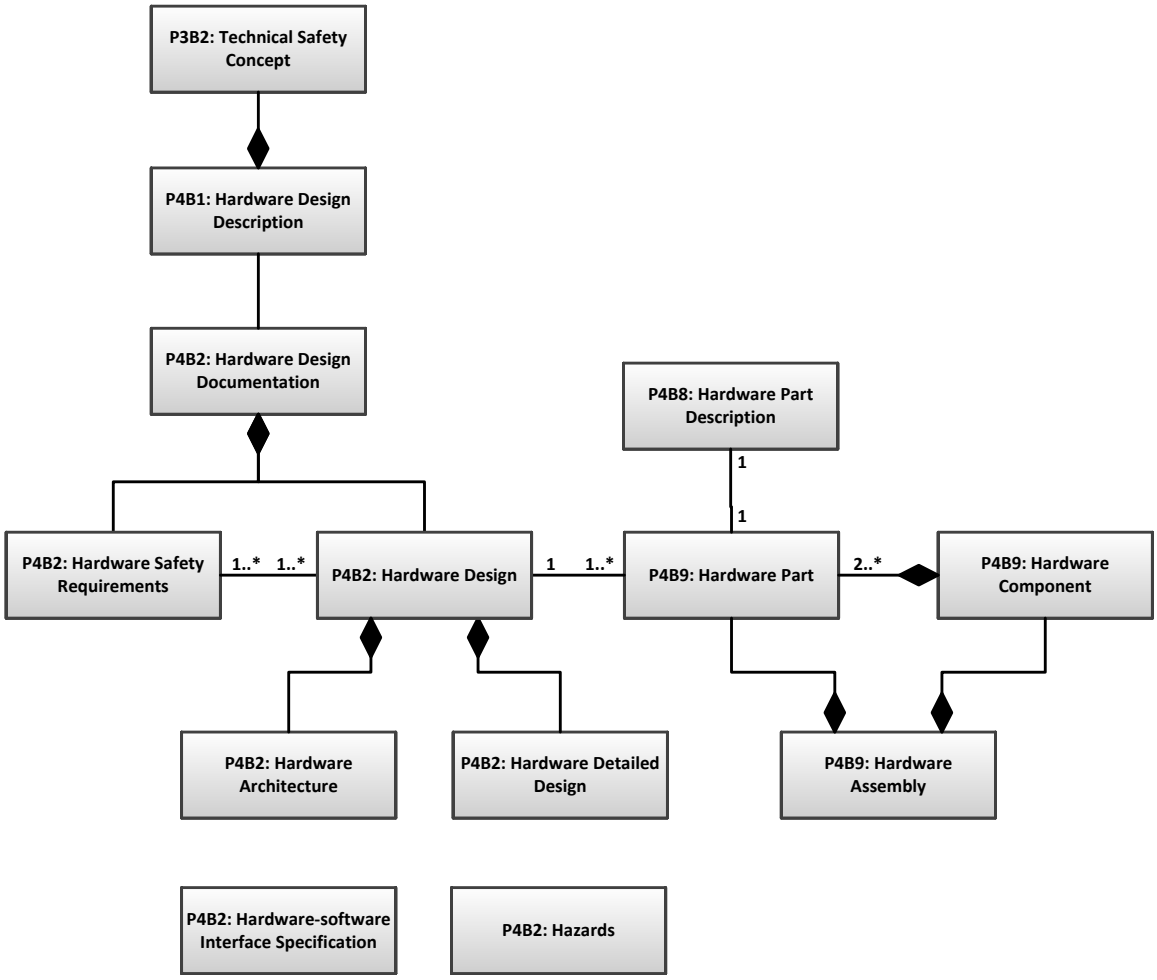

Figure 36: Pars 4 Hardware Design - Design Description, Design & Realisation

The model also shows instances of *B6: Aspect Cascaded to other Partes*. *P4B2: Hardware-software Interface Specification* represents the need for the *Hardware-software Interface* specification to remain consistent with both hardware and software design which necessitates a dialogue between the two *Partes*. In our model, changes to the document are cascaded to *Pars 3 System Design including the Technical Safety Concept*. *P4B6: Hazards* acknowledges that new hazards may be identified at any stage of the design process; they are most likely to be identified when establishing the properties of the design. Any hazards identified would be cascaded to *Pars 1 Item Definition and the Hazard Analysis and Risk Assessment*.

Physical Realisation

The hardware design is realised as a set of interconnected hardware parts or components, modelled here as *P4B9: Hardware Assembly*. ISO 26262 defines a hardware component, *P4B9: Hardware Component*, as being composed of two or more hardware parts and a hardware part, *P4B8: Hardware Part*, as being something which cannot be subdivided. As such, the *P4B9: Hardware Part Description* is associated with the hardware part. An ontology of typical hardware parts is

shown in Figure 37; this diagram models the software executable as being a part of the microprocessor.

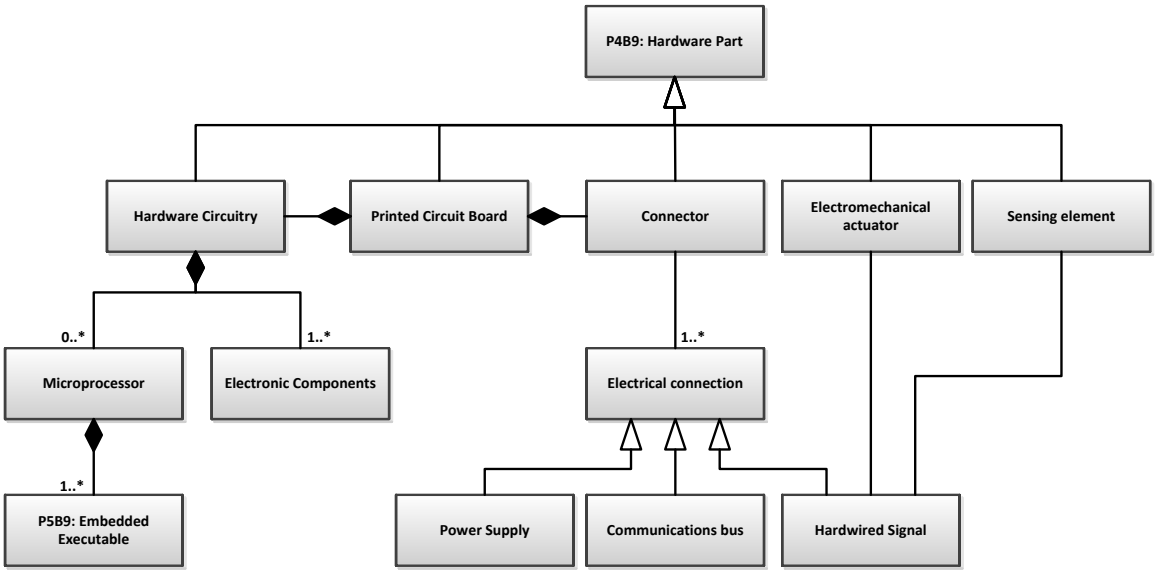

Figure 37: Ontology of Typical Hardware Parts

Design Properties

The design properties of *P4B2: Hardware Safety Requirements* required by ISO 26262 are that they are complete and consistent with regard to the *Technical Safety Concept*, the *Technical Safety Requirements*, the *System Design* and the *Hardware-software interface specification*. These properties are established by the use of review techniques listed in the standard.

The design properties of *P4B2: Hardware Design* required by ISO 26262 are that it is:

- consistent with the *Technical Safety Concept* and the *System Design*
- complete with respect to the *Technical Safety Requirements* allocated to the hardware
- compliant with the *Hardware Safety Requirements*
- consistent with the relevant *Software Safety Requirements*
- able to meet the *P3B2: Design target values for unmanaged random failures*

These properties are established by the use of review and analysis techniques listed in the standard.

Physical Realisation Properties

The property of *P4B9: Hardware Assembly* required by ISO 26262 is that it is a complete and correct of implementation of the *Hardware Safety Requirements*. This is established by the use of test techniques listed in the standard.

Safety Argument

The safety argument for the *Hardware Design Pars* is shown in Figure 38.

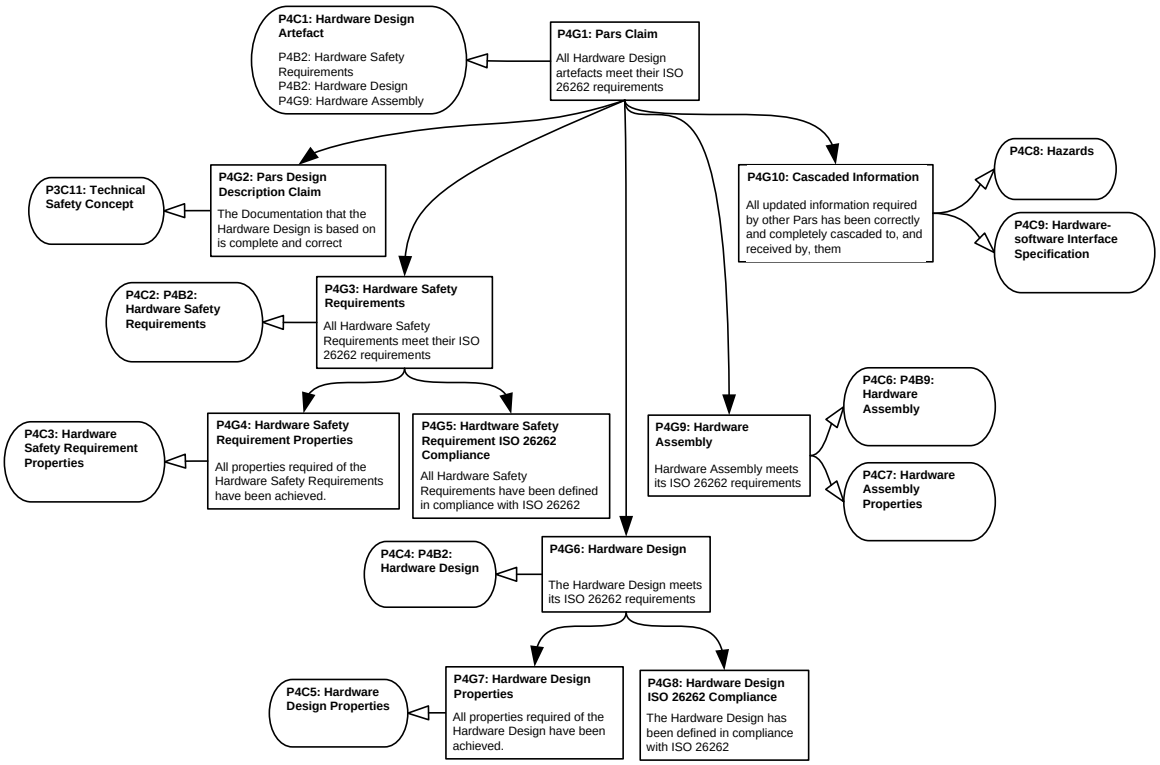

Figure 38: Hardware Design Pars Safety Argument

The argument is structured around the *Hardware Design* artefacts for which the claim, *P4G1*, is made that these meet all their ISO 26262 requirements. The *P4G2: Pars Design Description Claim* is a claim made on information cascaded from *Pars 3 System Design including the Technical Safety Concept*. If the *Pars 3* work is conducted by the same team as the *Pars 4* work, then the claim is the same as *P3G3* and *P3G6* claims. If this is not the case, then the claim is developed by arguing that the information has been correctly passed from one organisation to another.

Each design artefact-related claim has two sub-claims, one that the design artefact has been created in accordance with the requirements of ISO 26262 and the other that the design artefact achieves all the properties required by ISO 26262. To substantiate the first of these, further claims and supporting evidence will be based on compliance with the requirements of ISO 26262 for the appropriate ASIL value, including the correct use of ASIL decomposition. In terms of the MISRA framework these are *means* claims.

To substantiate the second of these, further claims and supporting evidence will be based on the use of verification techniques such as review and analysis. The claims will be that the required properties have been demonstrated and that the correct techniques have been used. The former correspond closely to the MISRA framework *rationale* claims. The latter will again be based on the compliance with the requirements of ISO 26262 for the appropriate ASIL value and correspond to the MISRA framework *means* claims.

The claim related to the realisation is *P4G9: Hardware Assembly*. To substantiate this, further claims and supporting evidence will be based on the use of test techniques. The claims will be that the required properties have been demonstrated and that the correct techniques have been used. The former correspond closely to the MISRA framework *satisfaction* claims because they concern the relationship between the safety requirements and the corresponding product artefacts. The latter will again be based on the compliance with the requirements of ISO 26262 for the appropriate ASIL value and correspond to the MISRA framework *means* claims.

The final claim, *P4G10*, relates to cascading information to other *Partes*. To substantiate this, further claims and supporting evidence will be based on how the information has been correctly passed from one organisation to another.

3.4.5 *Pars 5*: Software Design

The *Pars Software Design* diagram is shown in Figure 39.

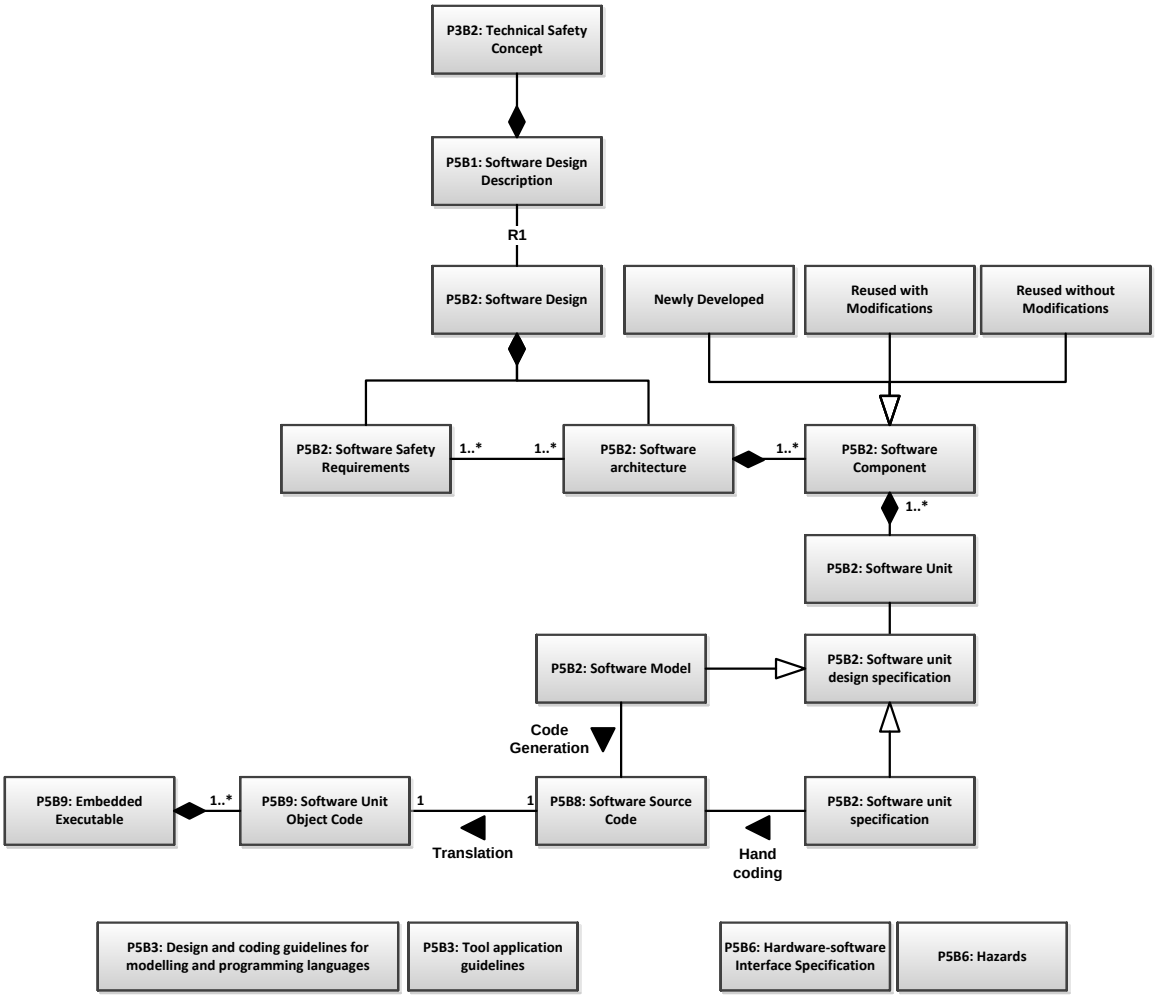

Figure 39: Pars 5 Software Design - Design Description, Design & Realisation

Design

The *B1: Pars Design Description* is instantiated as *P5B1: Software Design Description* and it consists of *P3B2: Technical Safety Concept* cascaded from *Pars* 3. The Technical Safety Concept is composed of the *System Design*, the *Technical Safety Requirements* assigned to elements of the system design, the *Hardware-software Interface* specification, the design target values for unmanaged random failures and the rationale underpinning the safety concept.

The *B2: Pars Design* is instantiated as *P5B2: Software Design* and it is composed of *P5B2: Software Safety Requirements* which are allocated to *P5B2: Software architecture*. The architecture is composed of *P5B2: Software Components* which ISO 26262 classifies as *Newly Developed*, *Reused with Modifications* or *Reused without Modifications*. Each software component is composed of *P5B2: Software Units* each of which has a *P5B2: Software unit design specification* which may take the form of a model, *P5B2 Software Model*, or a textual description, *P5B2 Software unit specification*. The source code, *P5B2 Source Code*, is either generated from the model or produced manually from the textual description. While the concept of a physical part description fits well with mechanical and electronic parts it is less obvious how to apply it in the software context. We have chosen to take the source code as an instance of *B8: Physical Part Description*.

In practice, the complete software architecture is made up of a variety of components, e.g. scheduler, communications, device drivers, middleware, and application algorithms, which are typically written by different organisations. Including them all in a single *Pars* is artificial but consistent with ISO 26262. The wide variety of actual approaches prohibits the creation of a generic model.

The model also shows instances of *B3: Pars Design Choice* required by ISO 26262, namely *P5B3: Design and coding guidelines for modelling and programming languages* and *P5B3: Tool application guidelines*.

The model also shows instances of *B6: Aspect Cascaded to other Partes*. *P5B6: Hardware-software Interface Specification* represents the need for the *Hardware-software Interface Specification* to remain consistent with both hardware and software design which necessitates a dialogue between the two *Partes*. In our model, changes to the document are cascaded to *Pars 3 System Design including the Technical Safety Concept*. *P5B6: Hazards* acknowledges that new hazards may be identified at any stage of the design process, they are most likely to be identified when establishing the properties of the design. Any hazards identified would be cascaded to *Pars 1 Item Definition and the Hazard Analysis and Risk Assessment*.

Physical Realisation

Source for each unit is translated (compiled) to object code corresponding to the unit. The final executable is created by linking together many unit object code files.

Design Properties

The design properties of *P5B2: Software Safety Requirements* required by ISO 26262 are that they are complete and consistent with regard to the *Technical Safety Concept*, the *Technical Safety Requirements*, the *System Design* and the *Hardware-software interface Specification*. These properties are established by the use of review techniques listed in the standard.

The design properties of *P5B2: Software architecture* required by ISO 26262 are that they are:

- Compliant with the *Software Safety Requirements* and the *Hardware-software Interface Specification*
- Robust against software and hardware failures (achieved by the use of safety mechanisms)
- Compliant with the rules of ASIL decomposition
- Compliant with the rules for freedom from interference when the architecture contains software components assigned different ASIL values
- Compatible with the target hardware

These properties are established by a combination of analysis and review techniques listed in the standard.

The design properties of *P5B2: Software unit design specification* required by ISO 26262 are that each:

- Fulfils the *Software safety requirements* allocated to it
- Is compliant with the *Hardware-software interface specification*

These properties are established by a combination of analysis and review techniques listed in the standard.

The design properties of *P5B2: Source Code* required by ISO 26262 are that it is:

- Compliant with its design specification
- Compliant with the coding guidelines (these are an instance of *B3: Pars Design Choice*)
- Compatible the target hardware

These properties are established by a combination of analysis and review techniques listed in the standard.

Physical Realisation Properties

The properties of each *P5B9: Software Unit Object Code* required by ISO 26262 are that they are:

- Compliant with the *Software unit design specification*
- Compliant with the *Hardware-software interface specification*

- Achieve the specified functionality
- Free from unintended functionality
- Robust against internal errors
- Execute within the resources that are available

These properties are established by the use of various testing techniques listed in the standard. The tests can be performed on a host or target processor.

The design properties for object code consisting of linked multiple instances of *P5B9: Software Unit Object Code* required by ISO 26262 are the same as for that of a single unit, except for *robust against internal errors*. Again, these properties are established by the use of various testing techniques listed in the standard. The tests can be performed on a host or target processor.

The properties of *P5B9: Embedded Executable* required by ISO 26262 are that it satisfies its requirements in the target environment. This is established by the use of various testing techniques listed in the standard and performed in the target environment.

Safety Argument

The safety argument for the *Software Design Pars* is shown in Figure 40.

The argument is structured around the *Software Design* artefacts for which the claim, *P5G1*, is made that these meet all their ISO 26262 requirements. The *P5G2: Pars Design Description Claim* is a claim made on information cascaded from *Pars 3 System Design including the Technical Safety Concept*. If the *Pars 3* work is conducted by the same team as the *Pars 5* work, then the claim is the same as *P3G3* and *P3G6* claims. If this is not the case, then the claim is developed by arguing that the information has been correctly passed from one organisation to another.

The claims related to the design artefact, (*P5G3*, *P5G6*, *P5G9*, *P5G12*), are all based on them meeting their corresponding ISO 26262 requirements and their further development is shown is Figure 41.

Each design artefact-related claim has two sub-claims: one that the design artefact has been created in accordance with the requirements of ISO 26262 and the other that the design artefact achieves all the properties required by ISO 26262. To substantiate the first of these, further claims and supporting evidence will be based on compliance with the requirements of ISO 26262 for the appropriate ASIL value, including the correct use of ASIL decomposition. In terms of the MISRA framework these are *means* claims.

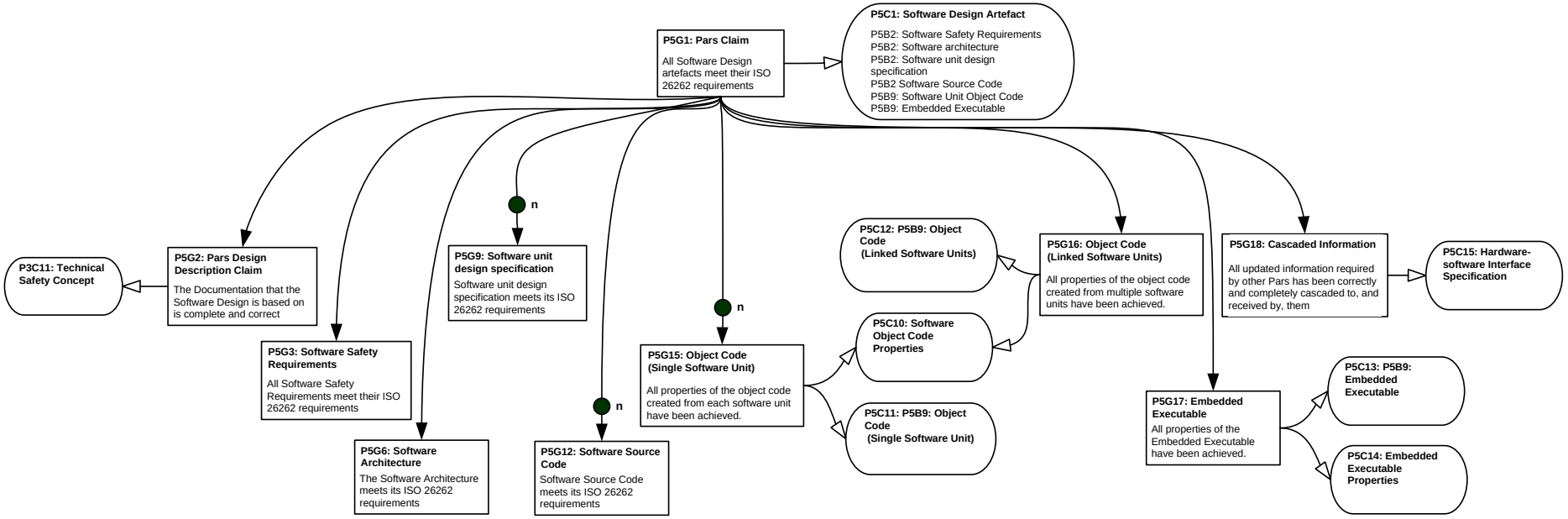

Figure 40: Software Design Pars Safety Argument 1

.

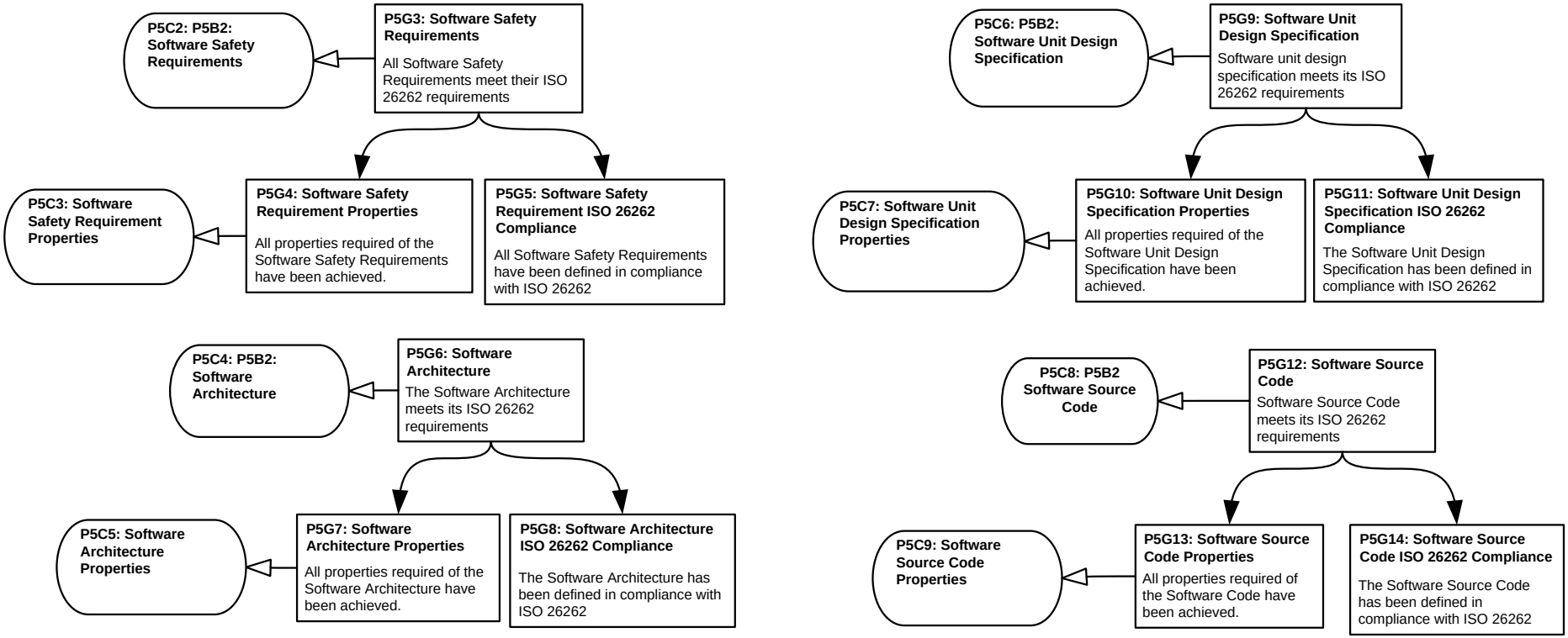

Figure 41: Software Design Pars Safety Argument 2

To substantiate the second of these, further claims and supporting evidence will be based on the use of verification techniques such as review and analysis. The claims will be that the required properties have been demonstrated and that the correct techniques have been used. The former correspond closely to the MISRA framework *rationale* claims. The latter will again be based on the compliance with the requirements of ISO 26262 for the appropriate ASIL value and correspond to the MISRA framework *means* claims.

The claims related to the realisation are *P5G15: Object Code (Single Software Unit)*, *P5G16: Object Code (Linked Software Units)* and *P5G17: Embedded Executable*. To substantiate these, further claims and supporting evidence will be based on the use of test techniques. The claims will be that the required properties have been demonstrated and that the correct techniques have been used. The former correspond closely to the MISRA framework *satisfaction* claims because they concern the relationship between the safety requirements and the corresponding product artefacts. The latter will again be based on the compliance with the requirements of ISO 26262 for the appropriate ASIL value and correspond to the MISRA framework *means* claims.

The final claim, *P5G18*, relates to cascading information to other *Partes*. To substantiate this, further claims and supporting evidence will be based on how the information has been correctly passed from one organisation to another.

3.4.6 Discussion

Although decisions may be made at one *Pars* about issues that are not strictly in the purview of that *Pars*, e.g. actuator selection in *Pars 1*, in the *Pars* structure their physical realisation is modelled in the appropriate *Pars*. In process terms, the work in *Pars 1* is an assumption that gets confirmed in work done later in another *Pars*, but the timing of the production of the material used in the *Pars* is not represented in the ontologies or argument.

In practice, work on nearly all the *Partes* starts at the same time and is performed concurrently. The *Pars* approach gives a way of showing this and making explicit the links. When starting, the information that has to be cascaded from another *Pars* will not always be available in a mature state, so work will be based on initial assumptions of tentative designs. This is similar to the ISO 26262 concept of a *Safety Element out of Context*.

The generic *B8: Physical Part Description* does not have any instances in the application to an *E/E system*. They would be part of a *rationale* claim supporting why a property had been achieved, i.e. because the part selected has a specification stating that the property is fulfilled.

The generic *B10: Related Physical Part* does not have any instances in the application to an *E/E system*. This because we did not consider the fitment of the ECU to the body of the vehicle as this is not a topic covered by ISO 26262.

3.5 Conclusion/Summary

We have presented a *design model* that can be used to represent the many different divisions, *Partes*, that an actual development may be split into. Using the *design model* as the basis, a safety argument pattern has been developed for a *Pars* which has the potential to facilitate the composition of an overall safety argument for the system from the arguments for each individual *Pars*.

We have illustrated that the design model can be applied to an *E/E system*, structured according to ISO 26262, and how the claims of the safety argument can be related to the requirements of ISO 26262. In Chapter 4 we investigate if the *design model* is general enough to be applied to a *mechatronic system*.

Chapter 4 Mechatronic Safety Argument

In Chapter 3 we described the *Pars* approach to partitioning the development of a system. This is based on a generic design ontology, process and design/safety argument pattern. We applied these ideas to an *E/E system*, based on the ISO 26262 standard, and showed how the design ontology and the safety argument pattern could be recast to reflect the design structure used by the standard.

In this chapter we show how the design ontology and safety argument pattern could be recast for a *mechatronic system*. We take a *mechatronic system* to consist of both the *mechanical system* being controlled and the *E/E system* that is controlling it. The addition of the mechanical design to the safety argument brings questions concerning both the form of the argument and what evidence could be available to support the argument. These are discussed in this chapter and the issue of evidence is addressed fully in Chapter 6.

In this chapter we give examples of mechatronic *design artefacts* which are taken from a previously developed *4 Corner Air Suspension System*. An example of how the *4 Corner Air Suspension System* safety argument could be represented using the *Pars* approach is given in Appendix C.

4.1 Example System: 4 Corner Air Suspension

The application of the *Pars* approach is illustrated by a system, *Four Corner Air Suspension*, (4CAS) that has been in production since 2004. This was chosen as it is a system well-known to the author. It has the classic characteristics of a *mechatronic system*, as described in section 2.3.1 Mechatronic Systems, and has typical *design artefacts* which are available, so it provides a good evaluation of the ontology. While the development of the 4CAS system predates the publication of the ISO 26262 standard, the concepts that ISO 26262 contains, which were largely based on IEC 61508, were applied to the development of the system.

The 4CAS material presented is based on that which was created at the time and is representative of what may actually be produced, given the nature of the system. Its use here shows to what extent it can be reinterpreted in the new structure. Much of the material has not been changed, while some diagrams have been redrawn to better reflect the division into *Partes*. The material is used as an example of what the content of the engineering artefacts of the different *Partes* may contain. It is not a complete description and serves only as an illustration for the design material. All of the safety argument diagrams have been created as part of the application of the *Pars* approach in the course of writing this thesis. Although the development of the *Pars* approach has been informed by working with the 4CAS example, the approach itself has been developed from the material in the literature review and in particular the ISO 26262 standard.

A brief description of the 4CAS system is now presented. The purpose of the 4CAS system is to provide the following primary customer features:

- Raise or lower vehicle body to predefined heights as selected by the user or dictated by vehicle handling constraints
- Maintain a level body at the selected vehicle height

It is also able to enhance vehicle performance when traversing rough terrain by allowing increased articulation of the front and rear wheels using a feature referred to as cross-linking.

These features are achieved by having an air spring at each of the four corners of the vehicle and using compressed air to independently increase or decrease the pressure in each air spring, thereby affecting the body ride height and inclination (forward-backwards and side-to-side). Height sensors at each corner allow closed loop control of the corner heights. Figure 42 shows a high-level Block Definition Diagram for 4CAS.

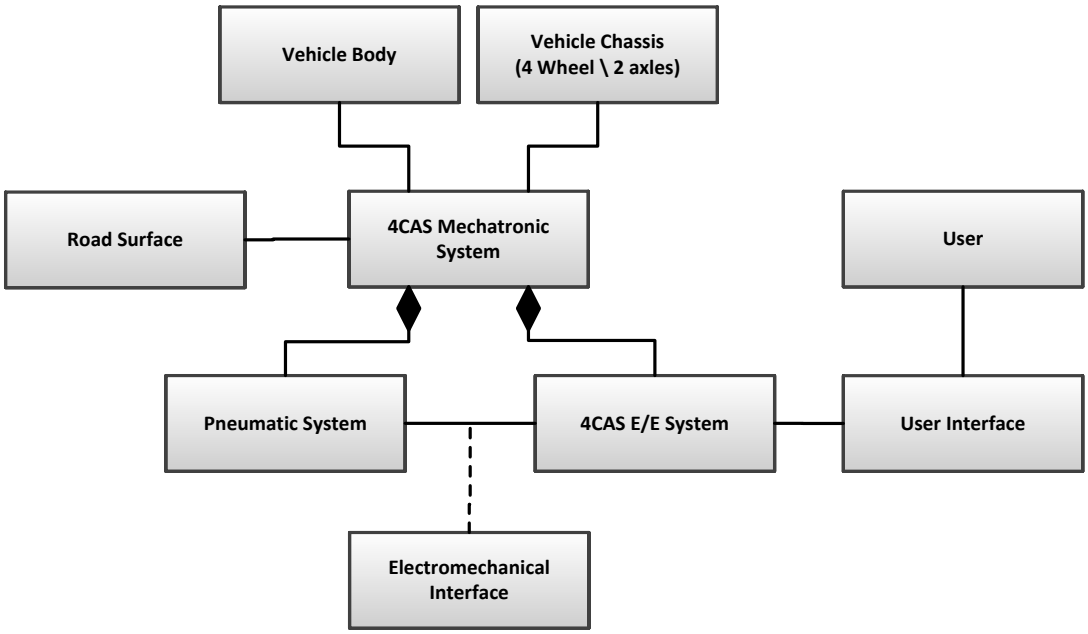

Figure 42: 4CAS High Level Block Diagram

The *Vehicle Body* is raised or lowered relative to the *Vehicle Chassis*. Lowering the vehicle makes ingress and egress easier for a vehicle that would otherwise be higher than a saloon vehicle. A high body position is advantageous for driver visibility, but when driving quickly a lower position reduces wind resistance and so improves fuel economy. When travelling off-road, a higher-than-usual body height gives more ground clearance which makes it possible to traverse uneven ground. In a passive suspension system the flatness of the body, with respect to the chassis, depends on the weight distribution within the vehicle. The 4CAS is able to maintain a flat body whatever the weight distribution. If the body is lowered to rest on the chassis, the ride comfort is directly dependent upon the road surface, i.e. very uncomfortable.

The *Pneumatic System* is controlled by the 4CAS ECU via an *Electromechanical Interface*, e.g. air compressor, valves. The 4CAS ECU consists of electronic hardware for reading inputs and driving the *Electromechanical Interface*, and a microprocessor executing software that controls the *Pneumatic System* so as to achieve the customer features. The *User Interface* allows the user to select ride heights via switches within the cabin and also via the smart key. The *User Interface* is provided by other vehicle systems and the user's requests are communicated over a network to the 4CAS ECU. If the vehicle starts to travel too fast at the off-road height, then the system will lower the ride height without a request from the driver.

4.2 Application of Pars Approach to a Mechatronic System

In the last chapter we partitioned the *E/E system* into five *Partes*. Here we define a set of seven *Partes* for a *mechatronic system* most of which are reused, sometimes with modification, from the *E/E system Partes*. In practice, the *Partes* covering the design would normally have further subdivisions, but we have restricted ourselves to these seven *Partes* so that the volume of documentation describing them is manageable. The seven *Partes* are:

- *Pars 1* Mechatronic Item Definition and the Hazard Analysis and Risk Assessment
- *Pars 2* Mechatronic Functional Safety Concept
- *Pars 3* Mechatronic Technical Safety Concept
- *Pars 4* E/E Technical Safety Concept
- *Pars 5* Hardware Design
- *Pars 6* Software Design
- *Pars 7* Mechanical Design

A revised version of Figure 29 showing the new relationship between the design and safety documentation for a *mechatronic system* is shown in Figure 43.

The *Item Definition* now explicitly includes the mechanical aspects, although in practice this is not much of a change from current practice as this document has always had to contain sufficient information about the plant being controlled to allow the hazard analysis to be performed. Consequently, the *Hazard Analysis* and *Risk Assessment* is the same for the *mechatronic system* as it was for the *E/E system*. Similarly, renaming the *Safety Goals* to *Mechatronic Safety Goals* is not a substantive change.

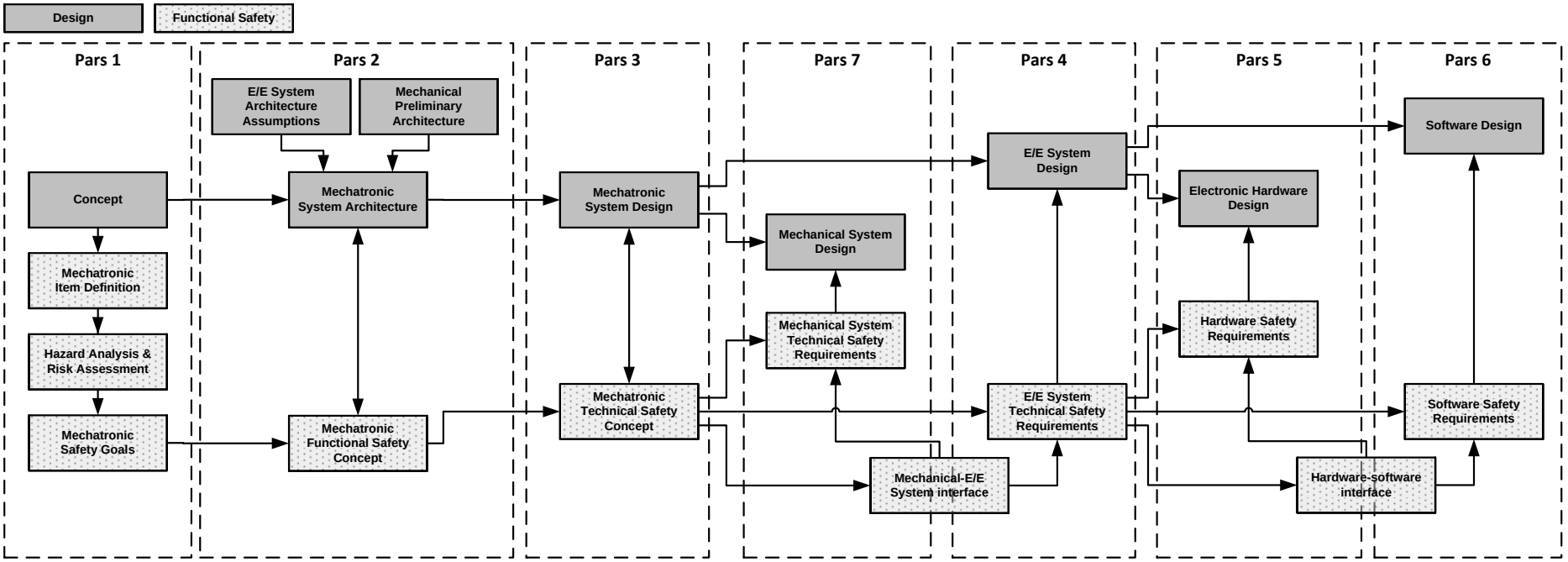

Figure 43: Mechatronic System Design & Safety Documentation

On the design side, the *Preliminary Architecture Assumptions* are replaced by the *mechatronic system* Architecture which is made up of both the *E/E system Architecture Assumptions* and the *Mechanical Preliminary Architecture*. The use of the words *Preliminary* and *Assumptions* allows for the fact that the initial stages of the safety process may be performed before the details of the design are decided. In the experience of the author, the design is usually quite mature and the main design decisions made when the initial stages of the safety process are performed. The *Functional Safety Concept* becomes the *Mechatronic Functional Safety Concept* with the main change being that any mechanical aspects related to the plant being controlled are now included in the concept rather than being referred to as *External Measures* achieved by *Other Technologies*. The definition of the *Mechatronic Functional Safety Concept* is still intended to be as far as possible independent of the details of the mechanical and *E/E system* design. The *Mechatronic Technical Safety Concept* is where the *Mechatronic Functional Safety Concept* gets mapped to the actual design and technical safety requirements are placed on the mechanical design and the *E/E system* design. The relationships between the requirements placed on the mechanical and *E/E system* design necessary to achieve the *Mechatronic Technical Safety Concept* are documented in the *Mechanical-E/E System* interface. From this point on, the development of the *E/E system* is unchanged.

Note: the use of the terms in the diagram are not intended to prescribe a particular set of documentation; rather they are used to communicate an idea. In practice, the information contained in these will be embedded in the document structure and supporting tools used by the organisation.

4.2.1 Pars 1 Mechatronic Item Definition and the HARA

The *Pars* 1 *mechatronic Item Definition* and the *Hazard Analysis* and *Risk Assessment* diagram is shown in Figure 44.

Although it has similarity with the equivalent one for an *E/E system,* its scope is now that of the complete *mechatronic system*. As discussed above, the *Initial System Description* now explicitly contains any relevant information concerning the mechanical design while the renaming of some of the blocks does not substantively change the content. The *E/E system* example acknowledged that hazards may also be identified in *System Design* and *Hardware Design Partes*; in the *Mechatronic System* example hazards may also be identified in the *Mechanical Design Pars*.

4CAS Example

The *Initial System Description* largely consists of the material presented in section 4.1. The *P1B1: Mechatronic Item Definition* lists the formal requirements, Table 8, which are modelled in a number of SysML *Use Case* diagrams which indicate the inputs necessary to achieve the required behaviour, see example in Figure 45, Figure 46 and Figure 47.

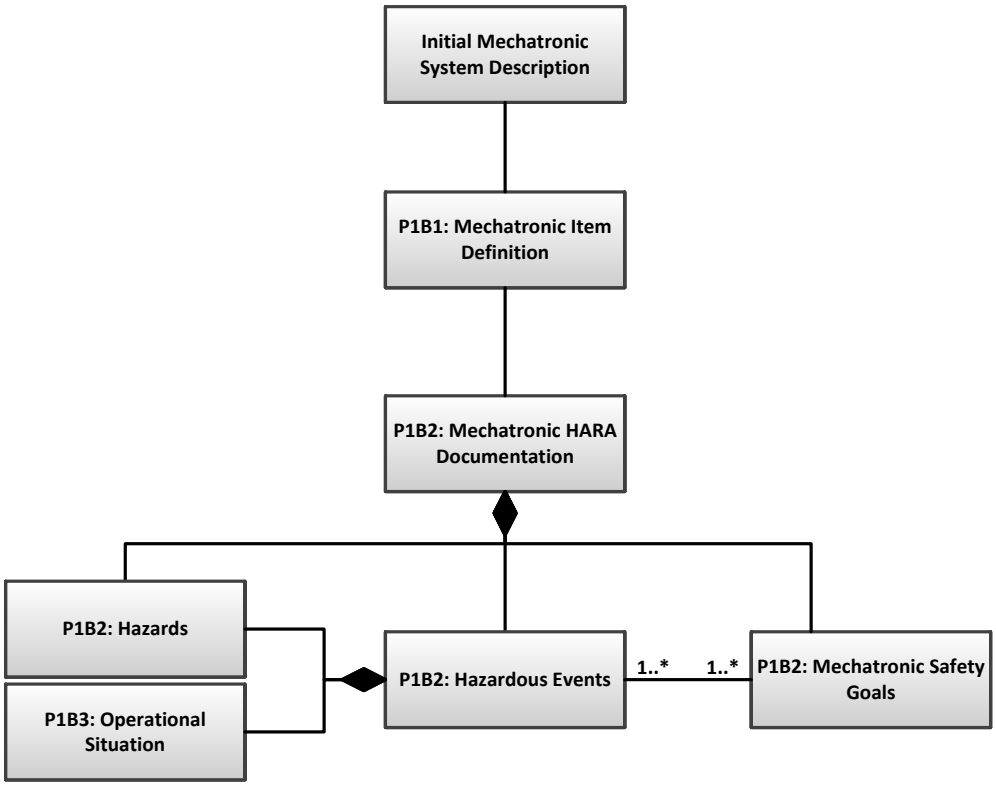

Figure 44: Pars 1 Mechatronic Item Definition HARA - Design Description and Design

Id	Requirement
NBSafReq_1	The Four Corner Air Suspension system shall control the quantity of air in the air springs at all four corners of the vehicle.
NBSafReq_2	The quantity of air in the air springs at all four corners of the vehicle shall be delivered in response to the height measured at the four corners using sensors.
NBSafReq_3	The Four Corner Air Suspension system shall maintain the target ride height under all rated vehicle operating conditions
NBSafReq_4	While the ignition is off, the system shall wake itself periodically to perform restricted levelling, also known as periodic levelling.
NBSafReq_5	The time intervals for the periodic levelling should be long enough to allow the system to cope with the length of time needed to identify considerable differences in corner heights.
NBSafReq_6	Vehicle height changes and corrections shall be restricted when any of the vehicle doors are open.
NBSafReq_7	The Four Corner Air Suspension system shall have selectable ride heights for different operating conditions.
NBSafReq_8	The driver shall be allowed to select one of the available ride heights by lowering or raising the air suspension using the in-car controls provided
NBSafReq_9	The driver controls may include for some vehicles a remote control
NBSafReq_10	The Terrain Response module may request height changes via the vehicle communications network.
NBSafReq_11	The 4CAS system will include different modes to inhibit some functionality during special procedures such as transportation and maintenance.
NBSafReq_12	The system shall detect conditions which imply loss of traction; therefore the system shall increase the quantity of air in the affected spring(s) to regain traction.
NBSafReq_13	The system shall detect conditions which imply the vehicle is lifting against an obstacle; therefore the system shall decrease the vehicle height or at least disallow raising the vehicle.
NBSafReq_14	Additional information about the air suspension system shall be displayed in the message centre
NBSafReq_15	The air suspension system shall be connected to the vehicle communications network.
NBSafReq_16	The air suspension system shall share some of its input and output signals with other vehicle systems using the vehicle communications network.

Table 8: 4CAS Item Definition Requirements

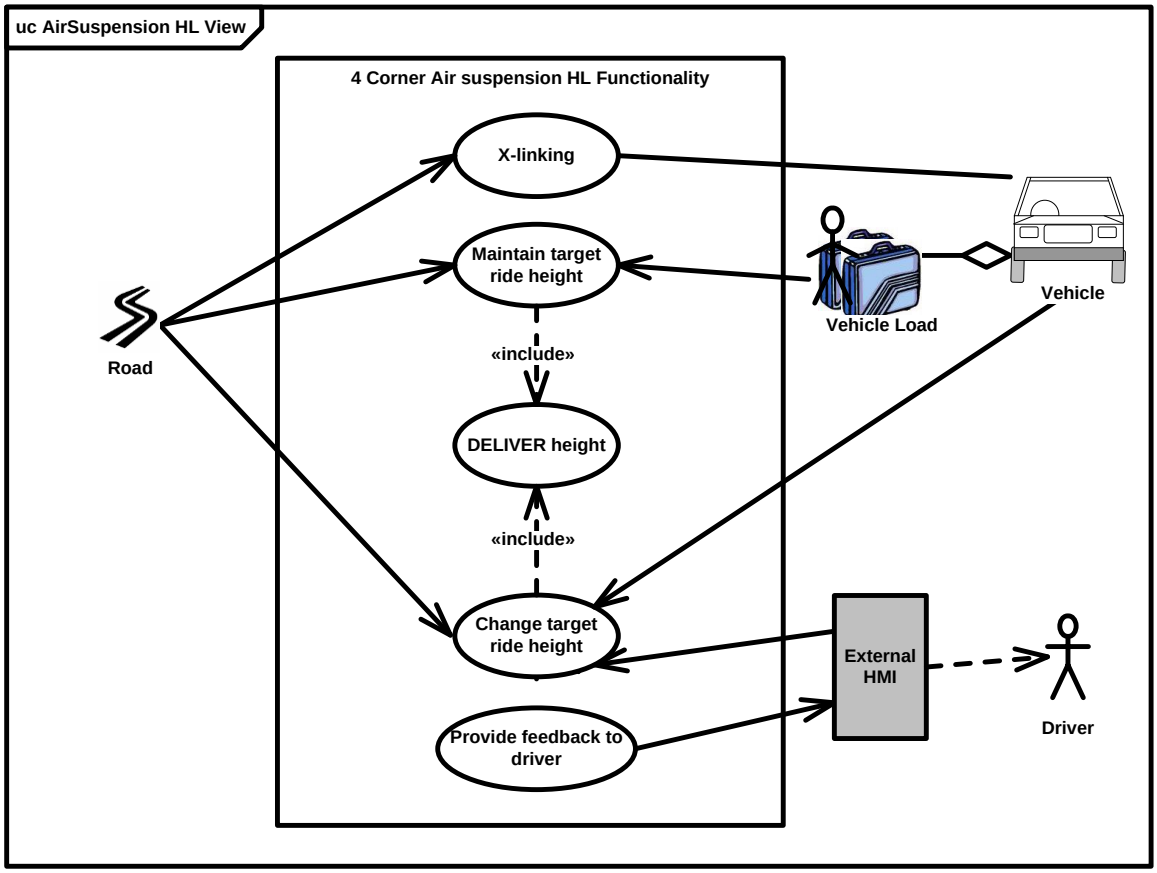

Figure 45: 4CAS Top Use Diagram

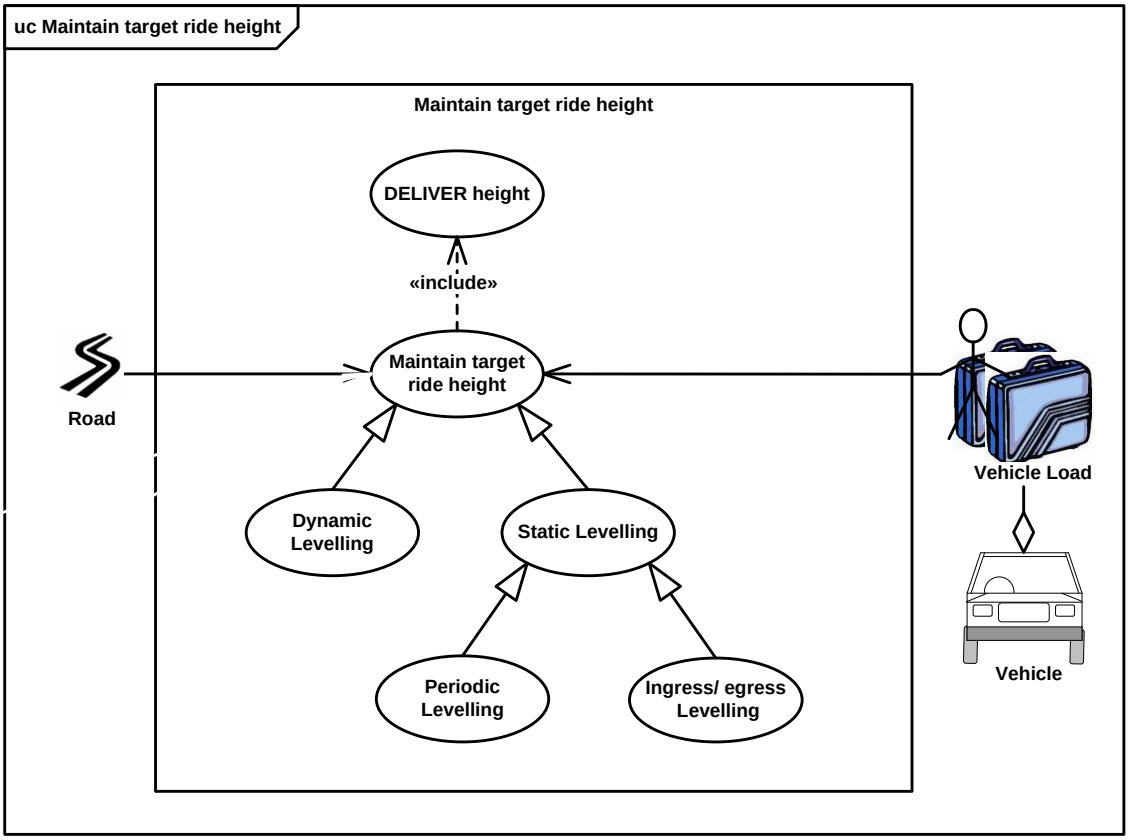

Figure 46: 4CAS Maintain Ride Height Use Case Diagram

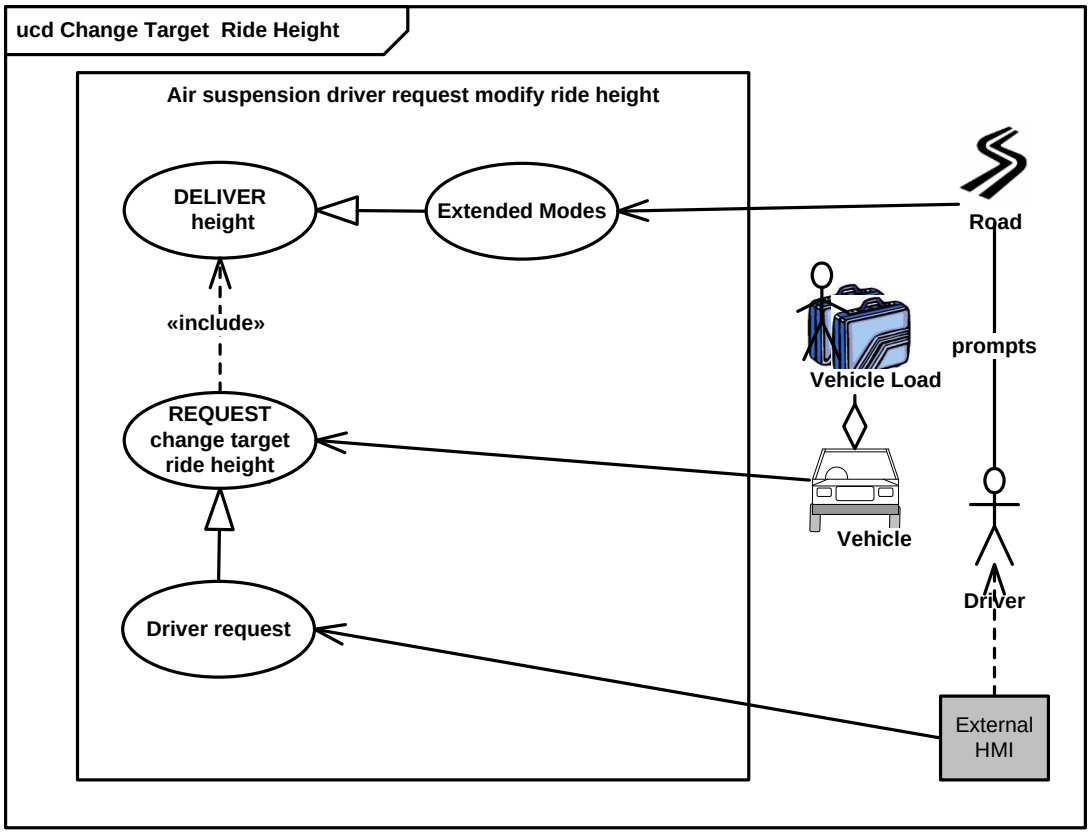

Figure 47: 4CAS Change Target Ride Height Use Case Diagram

Following the *hazard analysis* and *risk assessment*, a number of *Mechatronic Safety Goals* were defined, and examples are shown in Table 9.

Safety Goal 1	The vehicle occupants and other road users shall not be exposed to an unacceptable risk due to reduced resistance to roll over. (ASIL C)
Safety Goal 2	The vehicle users, and other road users, shall not be exposed to unacceptable risk due to gross height or pressure errors at the 4 corners. (ASIL B)
Safety Goal 3	People around the vehicle shall not be exposed to unacceptable risk due to the vehicle changing height. (ASIL QM)

Table 9: Example 4CAS Mechatronic Safety Goals

The instantiation of the argument pattern is shown in Figure 48. The pattern has not changed from the *E/E system* instantiation, the references to ISO 26262 have been retained as its *hazard analysis* and *risk assessment* process was always applicable to a *mechatronic system*. There has been some rewording to reflect the change of scope to a *mechatronic system*.

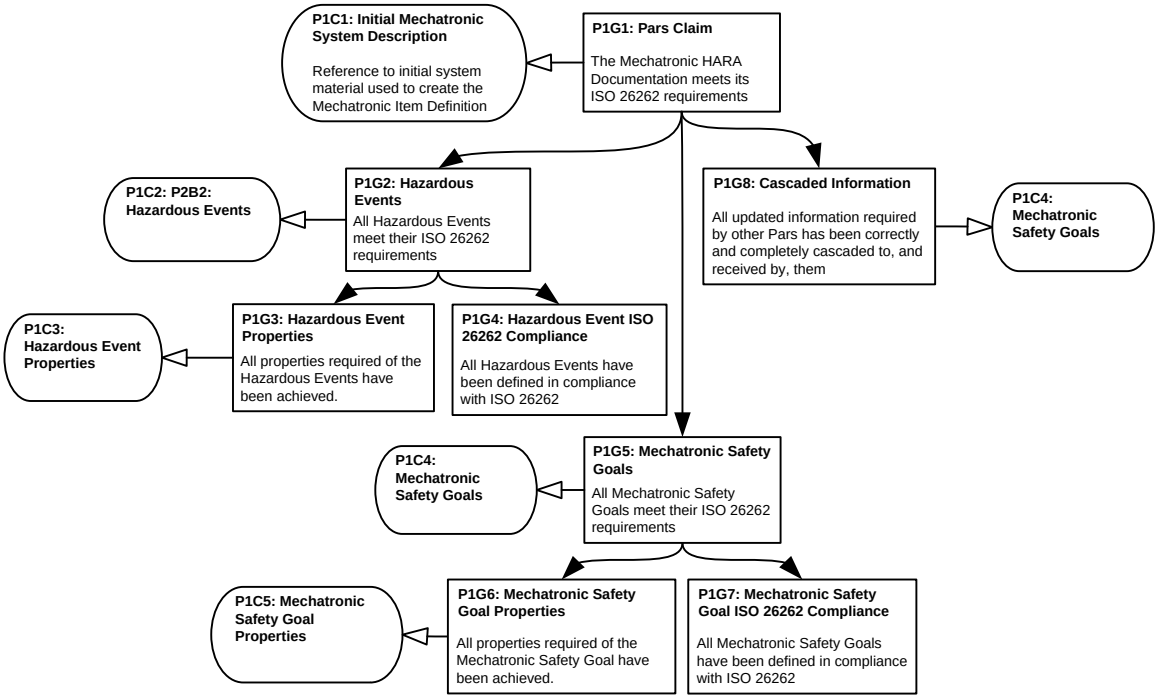

Figure 48: Pars 1 Mechatronic Item Definition and the HARA Safety Argument

4.2.2 Pars 2 Mechatronic Functional Safety Concept

The *Pars* 2 *Mechatronic Functional Safety Concept* diagram is shown in Figure 49.

Although the structure closely resembles that of the equivalent one for an *E/E system* with the blocks renamed, the content now reflects a complete *mechatronic system* design.

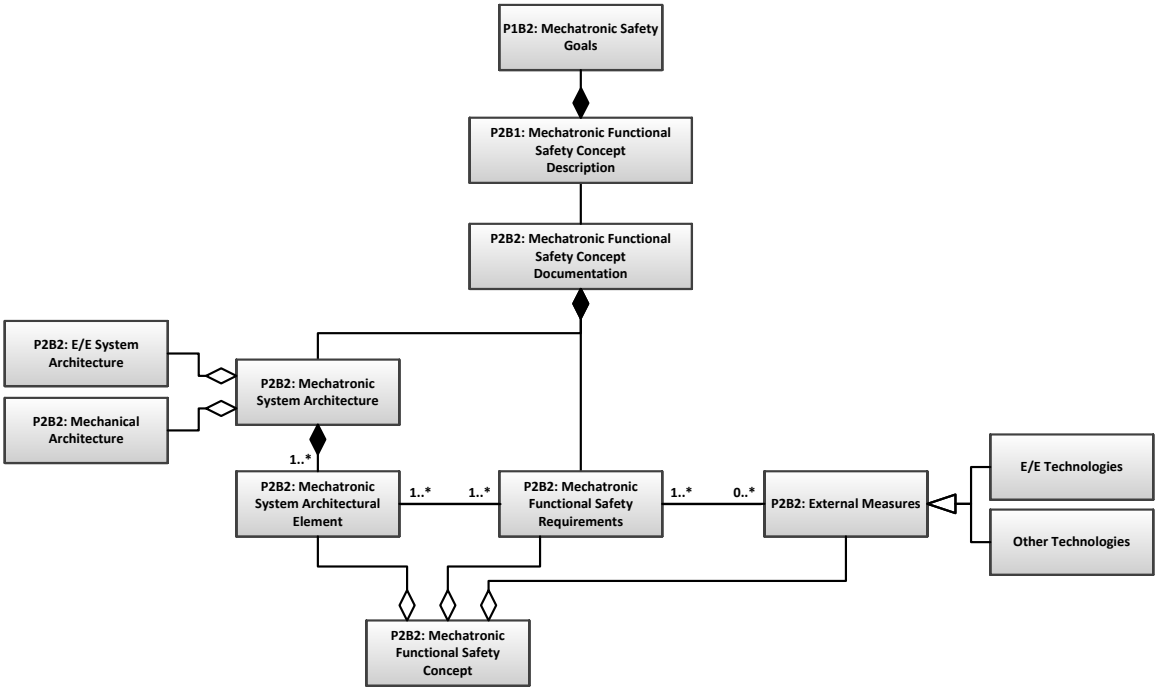

Figure 49: Pars 2 Mechatronic Functional Safety Concept - Design Description and Design

One change is that the *Mechatronic System Architecture* has to take account of both the *E/E system* and the *mechatronic system* shown here as *P2B2: E/E System Architecture* and *P2B2: Mechanical Architecture* respectively.

Another change is that for the *E/E system* the mechanical aspects were part of *External Measures*, whereas they are now part of the *Mechatronic System Architecture*. But the fact that *Functional Safety Requirements* are placed on mechanical elements of the design has not changed.

This does affect the design properties. The *Functional Safety Requirements* assigned to the E/E elements of the architecture also have an associated value of ASIL; this leads to design property *compliant with the rules of ASIL decomposition*. There ought to be something equivalent to this for the *Functional Safety Requirements* placed on the mechanical elements of the architecture, but this cannot be by means of an ASIL value. Here we note the problem and then address it in Chapter 6. The *External Measures* are still included, as there may be other mechanical or *E/E system* measures that are outside the scope of the *Item* that are included in the *Mechatronic Functional Safety Concept*.

It is *P2B2: Mechatronic Functional Safety Concept* that is cascaded to the *Pars 3*, *Mechatronic Technical Safety Concept*, and as such represents an instance of *B6: Aspect Cascaded to other Partes*.

4CAS Example

The 4CAS *E/E System Architecture* are shown in Figure 50.

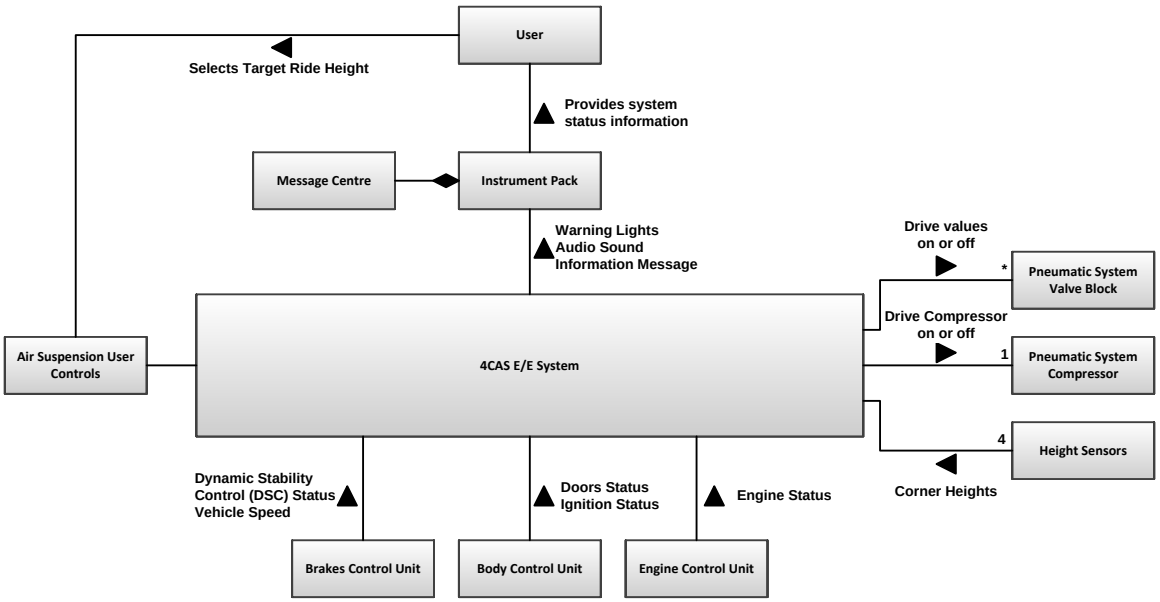

Figure 50: 4CAS E/E System Architecture Assumptions

The 4CAS *Mechanical Architecture* is shown in Figure 51

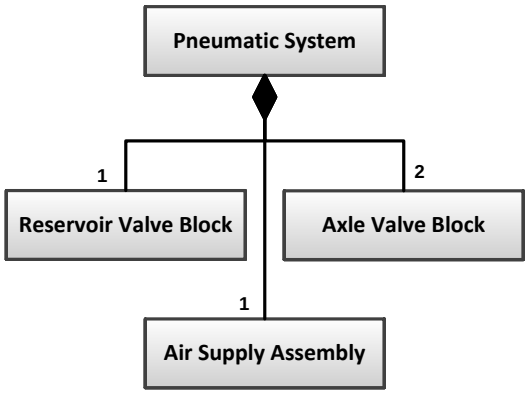

Figure 51:4CAS Mechanical Architecture

The operation of the 4CAS system was further defined by creating SysML *Activity Diagrams* to the required behaviour for the previously defined *Use Cases*, for example see Figure 52and Figure 53.

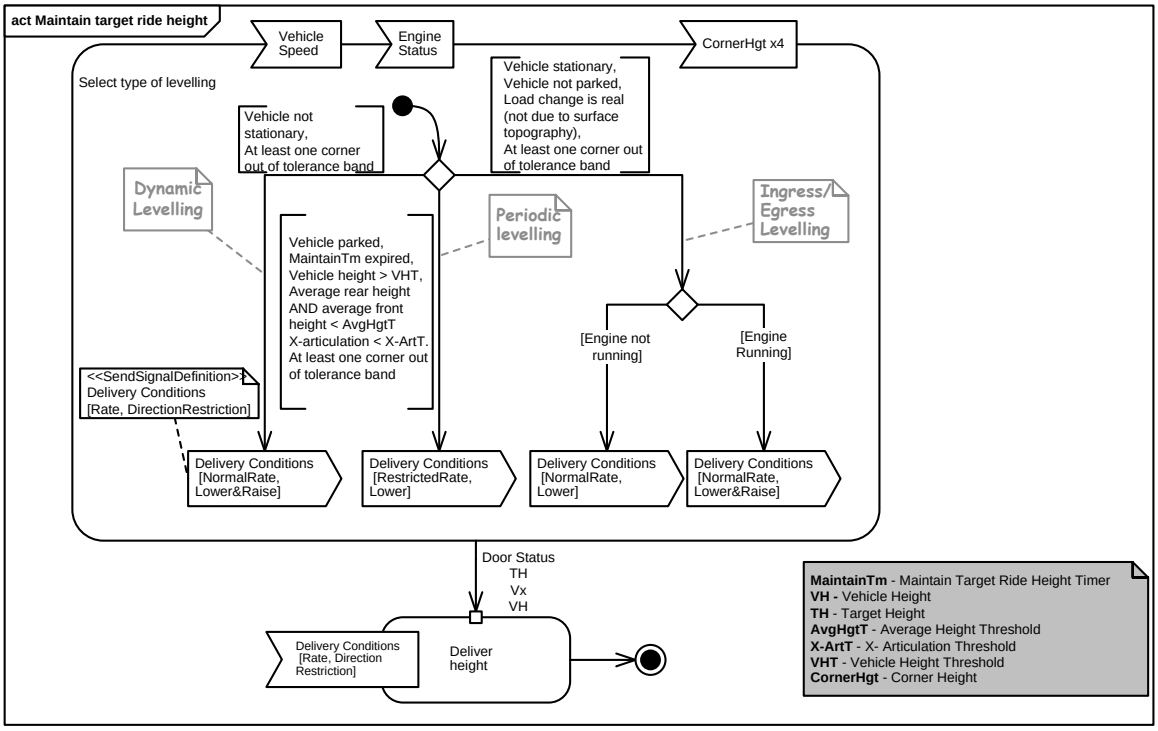

Figure 52: Activity Diagram for Maintain Ride Height Use Case

To develop the *Mechatronic Functional Safety Concept*, potential causes of failures of the activity diagrams were analysed and fault management requirements were derived to manage these failures such that the *Mechatronic Safety Goals* are not violated. These were expressed as a further set of *Activity Diagram*s, see example in Figure 54, Figure 55 and Figure 56.

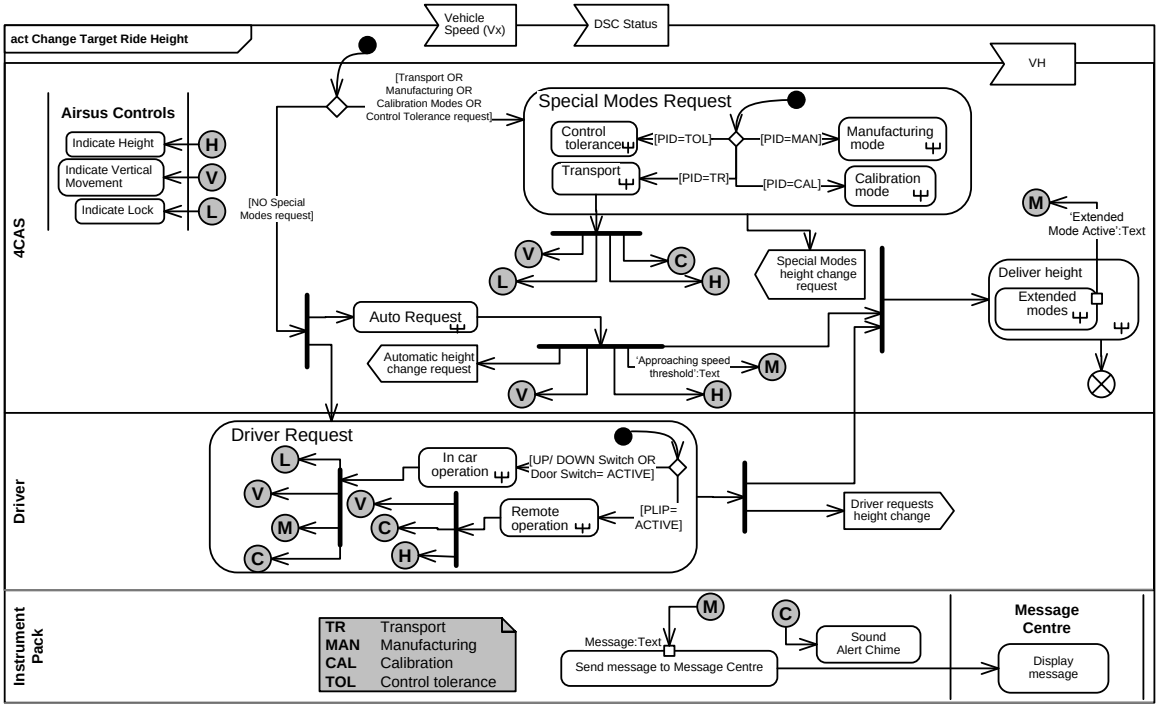

Figure 53: Activity Diagram for Change Target Ride Height

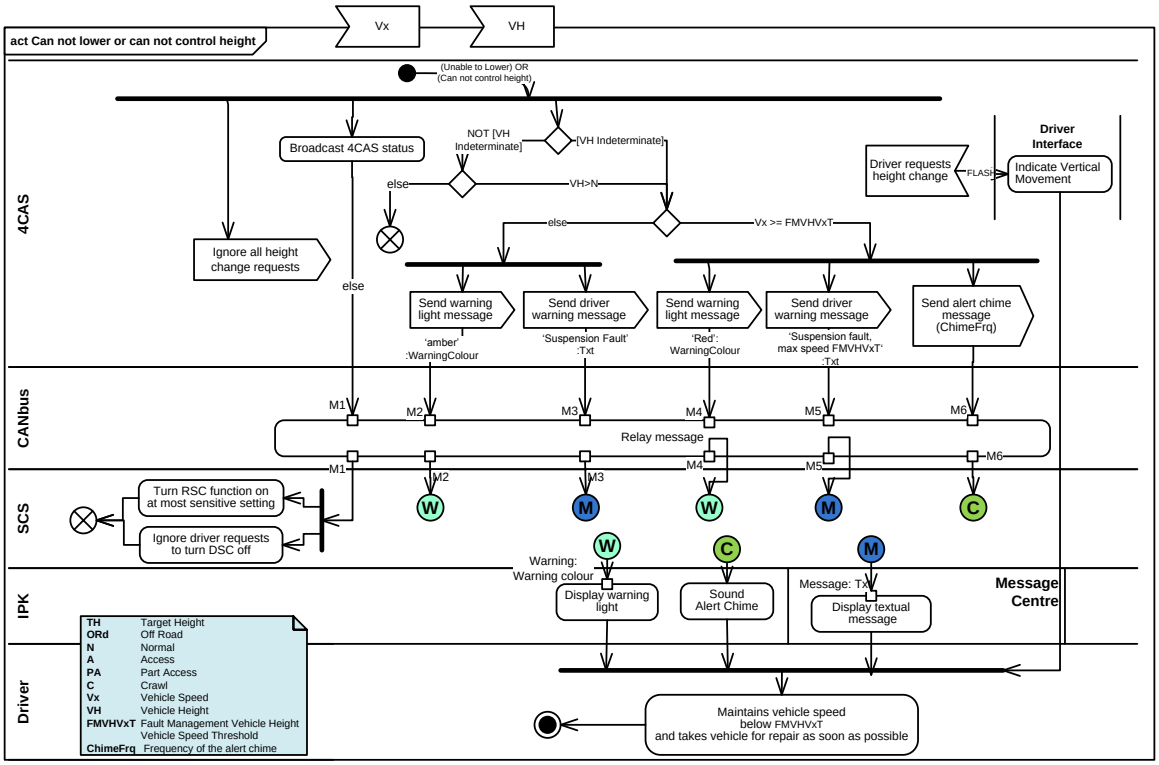

Figure 54: Fault Management Activity Diagram for Height Control Fault

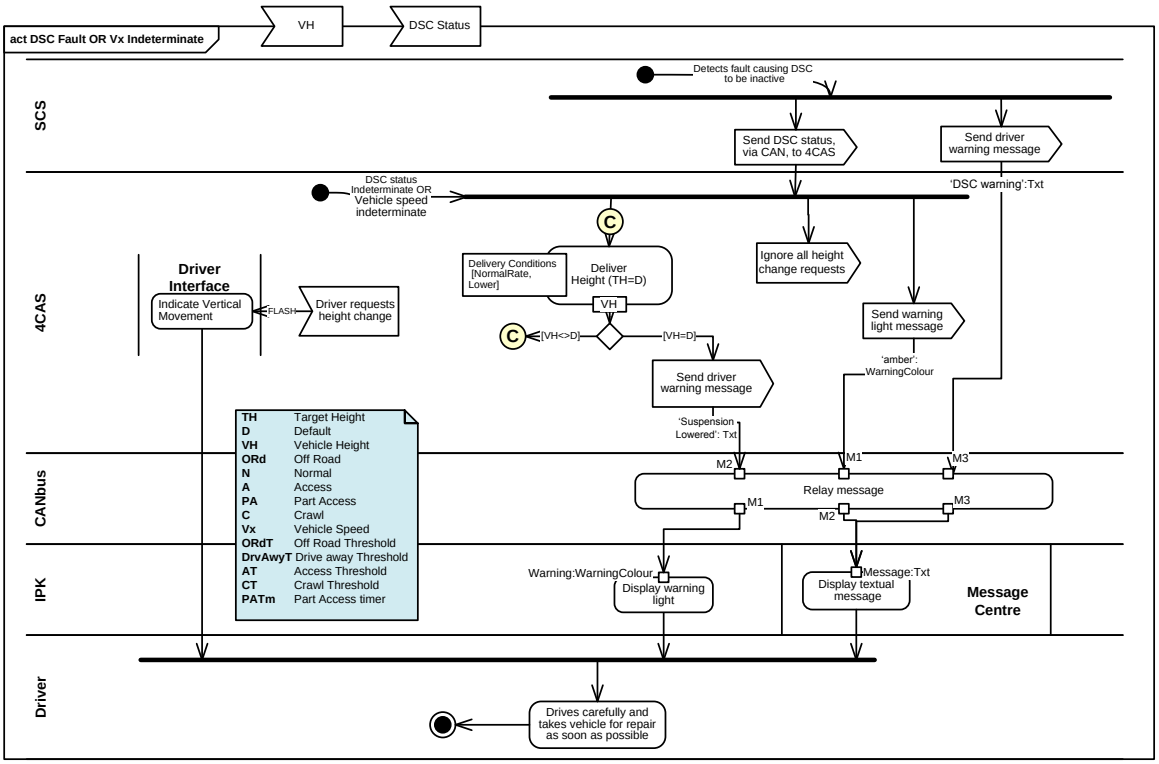

Figure 55: Fault Management Activity Diagram for Vehicle Speed or DSC Fault

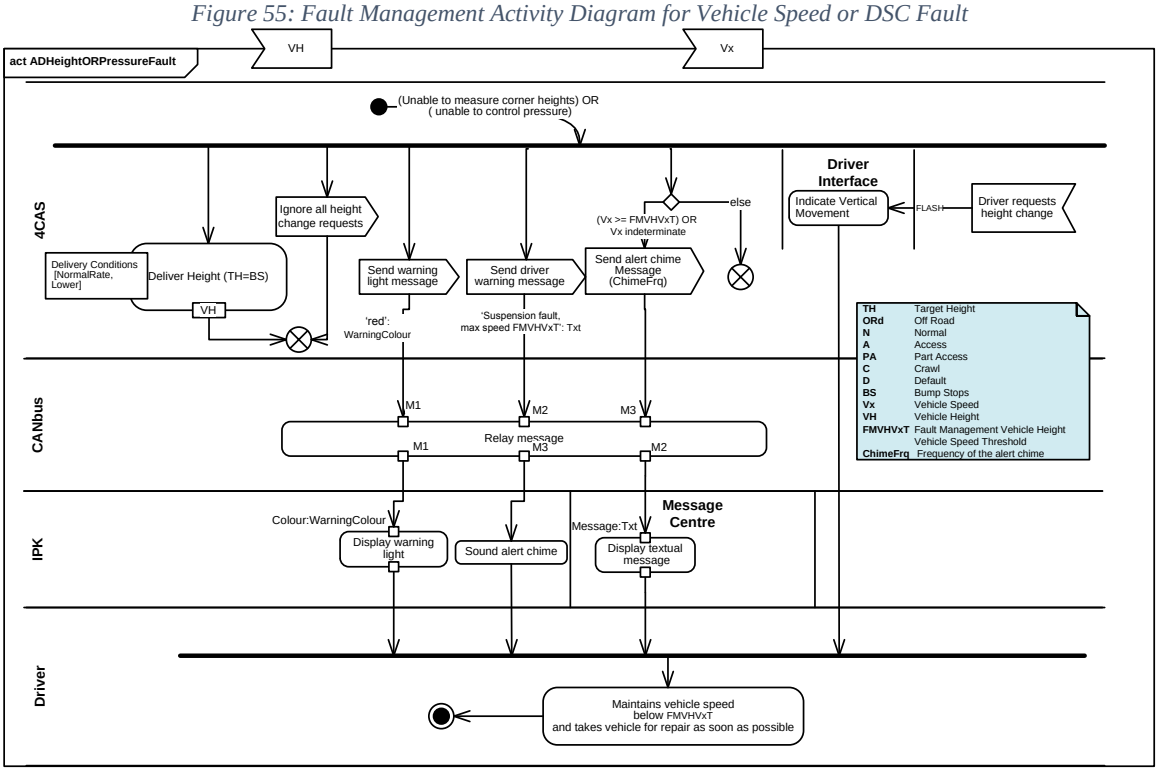

Figure 56: Fault Management Activity Diagram for Height or Pressure Fault

The instantiation of the argument pattern is shown in Figure 57. The pattern has not changed from the *E/E system* instantiation; there has been some rewording to reflect the change of scope to a *mechatronic system*.

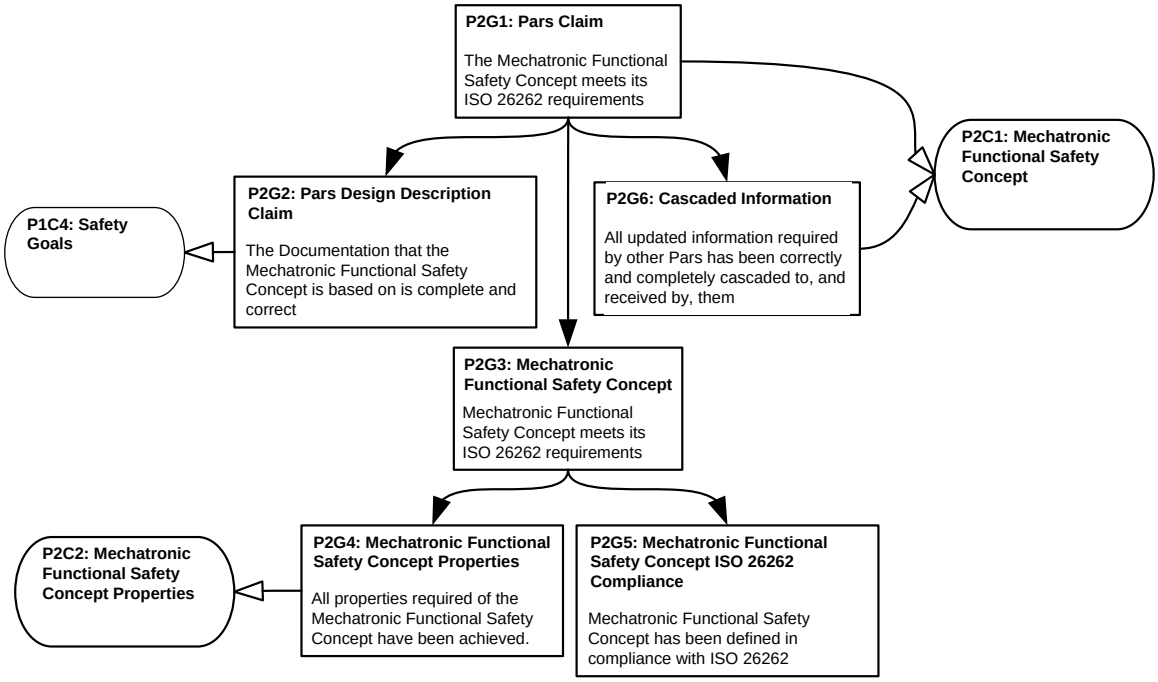

Figure 57: Pars 2 Mechatronic Functional Safety Argument

4.2.3 Pars 3 Mechatronic Technical Safety Concept

The *Pars* 3 *Mechatronic Technical Safety Concept* diagram is shown in Figure 58. This is a new *Pars* and is necessary to explicitly address the design of a *mechatronic system* which now explicitly includes mechanical elements.

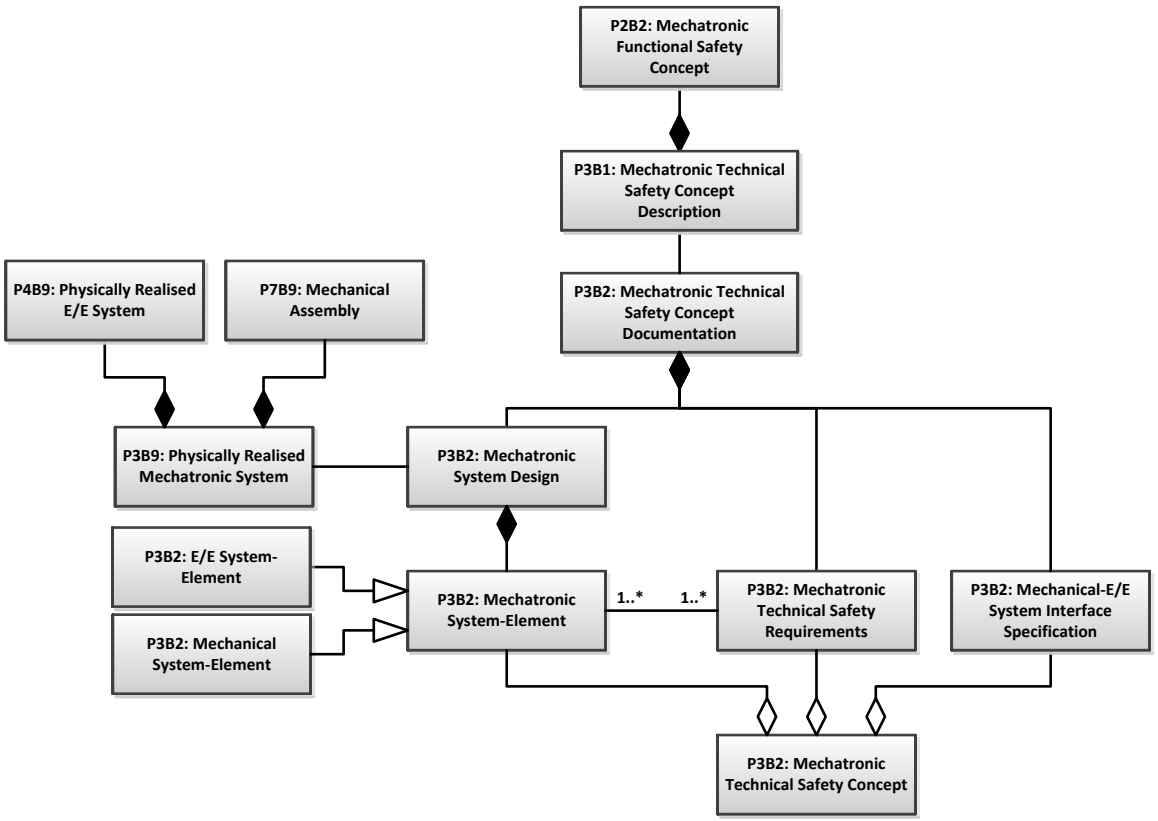

Figure 58: Pars 3 Mechatronic TSC - Design Description, Design & Realisation

Design

The *B1: Pars Design Description* is instantiated as *P3B1: Mechatronic Technical Safety Concept Description* and consists of *P2B2: Mechatronic Functional Safety Concept* cascaded from *Pars* 2. The Mechatronic Functional Safety Concept is composed of the *mechatronic system* architecture, the *Mechatronic Functional Safety Requirements* assigned to elements of the architecture, the *External Measures* and the rationale underpinning the safety concept.

The *B2: Pars Design* is instantiated as *P3B2: Mechatronic Technical Safety Concept Documentation* and it is composed of *P3B2: Mechatronic System Design*, *P3B2: Mechatronic System-Element*, *P3B2: Mechatronic Technical Safety Requirements* and *P3B2: Mechanical-E/E System Interface Specification*.

The Mechatronic Technical Safety Requirements, *P3B2: Mechatronic Technical Safety Requirements*, are allocated to elements of the system design, *P3B2: Mechatronic System-Element*. The *mechatronic system* design is a design choice and so also an instance of *B3: Pars Design Choice*. The system elements may be either *E/E system* elements or *mechatronic system* elements. The *E/E system* elements have integrity requirements associated with them in the form of an ASIL value. The meaning of the ASIL is delineated through the ISO 26262 standard, as the standard does not apply to mechanical elements of the design; the assignment of an ASIL value to a mechanical element has no meaning and is deprecated by ISO 26262. However, the concept of *desired integrity*, given the risk associated with failure, is still a valid concept for the mechanical elements. This issue is discussed further in chapter 6.

The interface between the two different types of element is documented in the interface specification, *P3B2: Mechanical-E/E System Interface Specification*. The interface specification documents the interface between the *E/E system* and the *mechanical system*. This mediated by electromechanical actuators and sensing elements. The *mechatronic design* has to take into account mechanical, hardware and software factors. For example, when considering the design of the actuators, there will be mechanical considerations of size needed to achieve the desired effect; these will have implications for the electronic drive circuitry in terms of voltage, current and power dissipation and also on the software in terms of response times required.

Following the approach that was used in the *E/E system* example, the *Mechatronic Technical Safety Concept* embodies the *Mechatronic Technical Safety Requirements* assigned to *E/E system* or *mechanical system* elements, their allocation and the design rationale. It is *P3B2: Mechatronic Technical Safety Concept* that is cascaded to the *E/E System Technical Safety Concept and Mechanical Design Partes* and as such represents an instance of *B6: Aspect Cascaded to other Partes*.

Physical Realisation

The *System Design* is implemented by *E/E system* elements and *mechanical system* elements realised in the E/E System Technical Safety Concept *Pars* and the *Mechanical Design Pars*. The realised *Mechatronic System Design* is represented by *P3B9: Physically Realised Mechatronic System* and is composed of *P4B9: Physically Realised E/E System* and *P7B9: Mechanical Assembly* from the *E/E System Technical Safety Concept Pars* and the *Mechanical Design Pars* respectively.

Design Properties

In the *E/E system* example we were able to take the required properties from the ISO 26262 standard. While there is not an equivalent standard for *mechatronic systems*, we can reasonably reapply some of the ISO 26262 properties to the *Mechatronic Technical Safety Concept*.

The design properties required of *P3B2: Mechatronic Technical Safety Requirements* could reasonably be stated as:

- compliant and consistent with the *Mechatronic Functional Safety Concept*
- compliant with the *Mechatronic System Design*
- compliant with the rules of ASIL decomposition for *P3B2: E/E System-Element*

These properties could be established by the use of review techniques in a similar way as for the *E/E system*. We have the recurrent problem of how to handle the integrity value for the *P3B2: Mechanical System-Element* given that it cannot be assigned an ASIL value.

The design properties required of *P3B2: Mechatronic System* could reasonably be stated as:

- compliant and complete with regard to the *Mechatronic Technical Safety Concept*
- robust against the causes of systematic failures and the effects of systematic faults

These properties could be established by the use of review, simulation and analysis techniques in as similar way as for the *E/E system*.

Physical Realisation Properties

Again, we can reasonably reapply some of the ISO 26262 properties to the *Mechatronic Technical Safety Concept*.

The properties design properties of *P3B9: Physically Realised Mechatronic System* could reasonably be stated as:

- compliant with *Mechanical-E/E System Interface Specification*
- correctly implements the *Mechatronic Functional and Technical Safety Requirements* and achieves the *safety goals* when operating as an Item in a vehicle in the context of the electrical architecture with other controllers

In practice, the achievement of the *safety goals* at the vehicle level is the same as for the *E/E System Technical Safety Concept* which are an assessment of:

- the controllability risk parameter under failure conditions when the system is fulfilling the *Functional and Technical Safety Requirements*
- the effectiveness of safety measures for controlling random and systematic failures
- the effectiveness of the external measures
- the effectiveness of the elements of other technologies

These properties could be established by the use of test techniques in a similar way as for the *E/E system*.

4CAS Example

The high level *4CAS Mechatronic System Design* is shown in Figure 59. This shows the breakdown of physical parts with the sensors and actuators being shown as part of the *E/E system*. External interfaces are not included on this diagram.

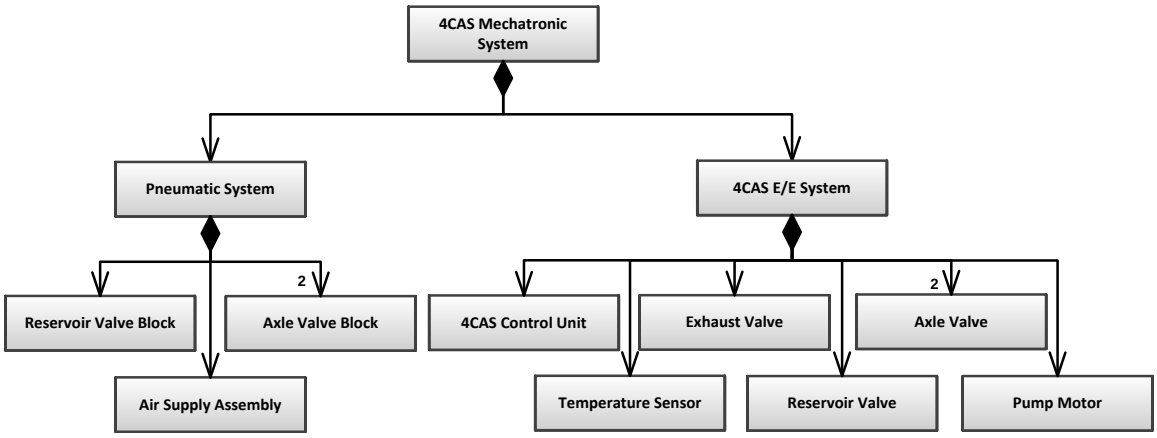

Figure 59: 4CAS Mechatronic System Design

The interface between the components shown in Figure 59 is specified in Figure 60.

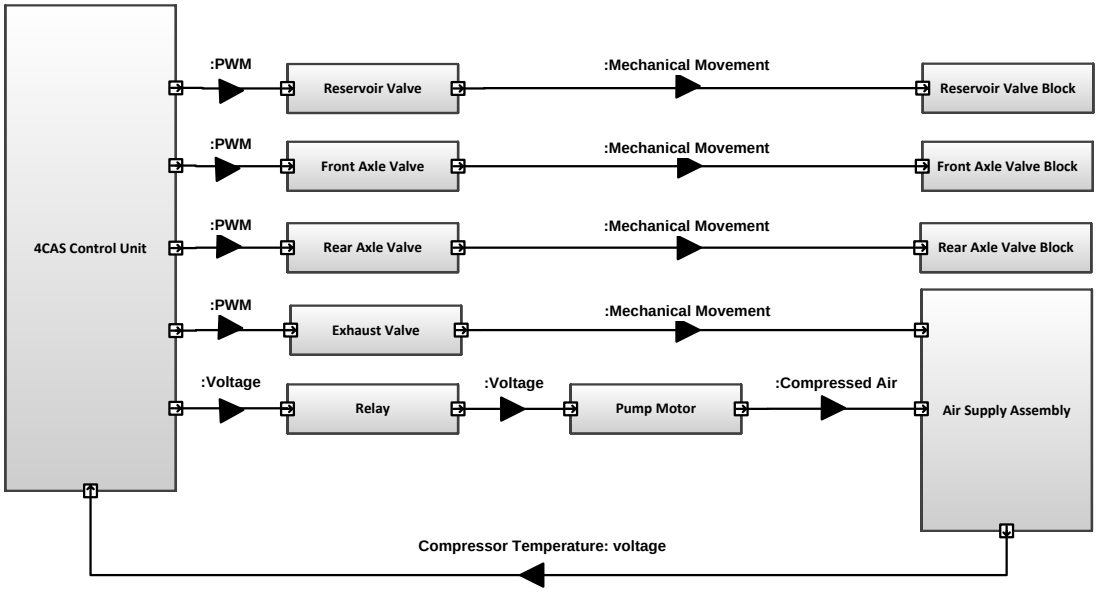

Figure 60: 4CAS Mechanical-E/E System interface

The interface specification contains details of the electrical specification of the valves, relay and pump and how they have to interface with the valve blocks and air supply assembly. The mounting of the valves is the responsibility of the mechanical design.

Safety Argument

The instantiation of the argument pattern is shown in Figure 61. The pattern is similar to the *E/E system* instantiation. However, as the properties of the artefacts are no longer defined by ISO 26262 some of the claims refer to the processes defined in *contexts* but these have not been instantiated.

4.2.4 Pars 4: E/E System Technical Safety Concept

The *Pars* 4 E/E *System Technical Safety Concept* diagram is shown in Figure 62. It is not substantially changed from the equivalent one for an *E/E system*. Some of the blocks have been renamed, Table 8, but the content has not changed. The model also shows instances of *B6: Aspect Cascaded to other Partes*. *P4B2: Mechanical-E/E System Interface Specification* represents the need for this specification to remain consistent with both *E/E system* design and *mechatronic system* design which necessitates a dialogue between the two *Partes*. In our model, changes to the document are cascaded to *Pars 3 Mechatronic the Technical Safety Concept*.

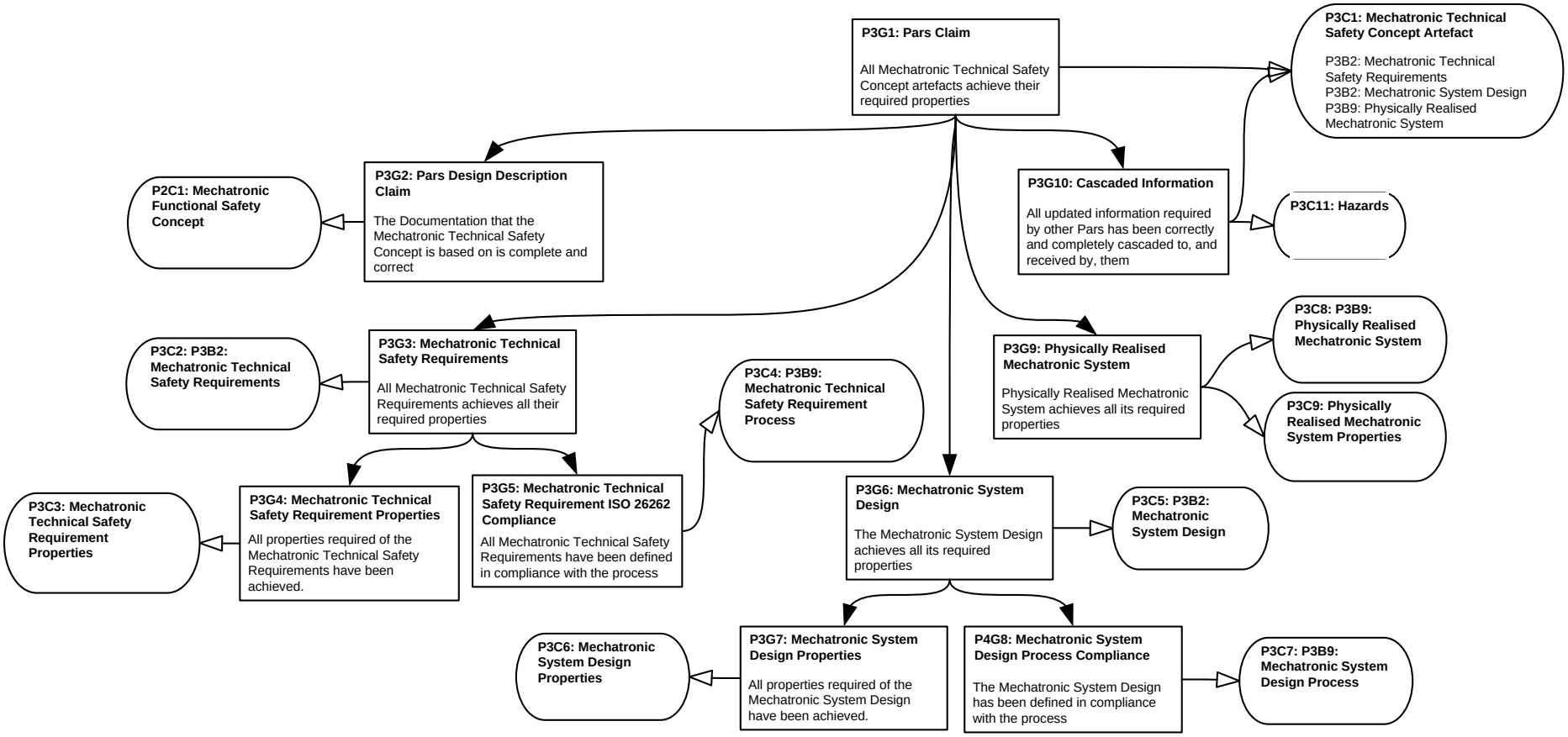

Figure 61: Pars 3 Mechatronic Technical Safety Argument

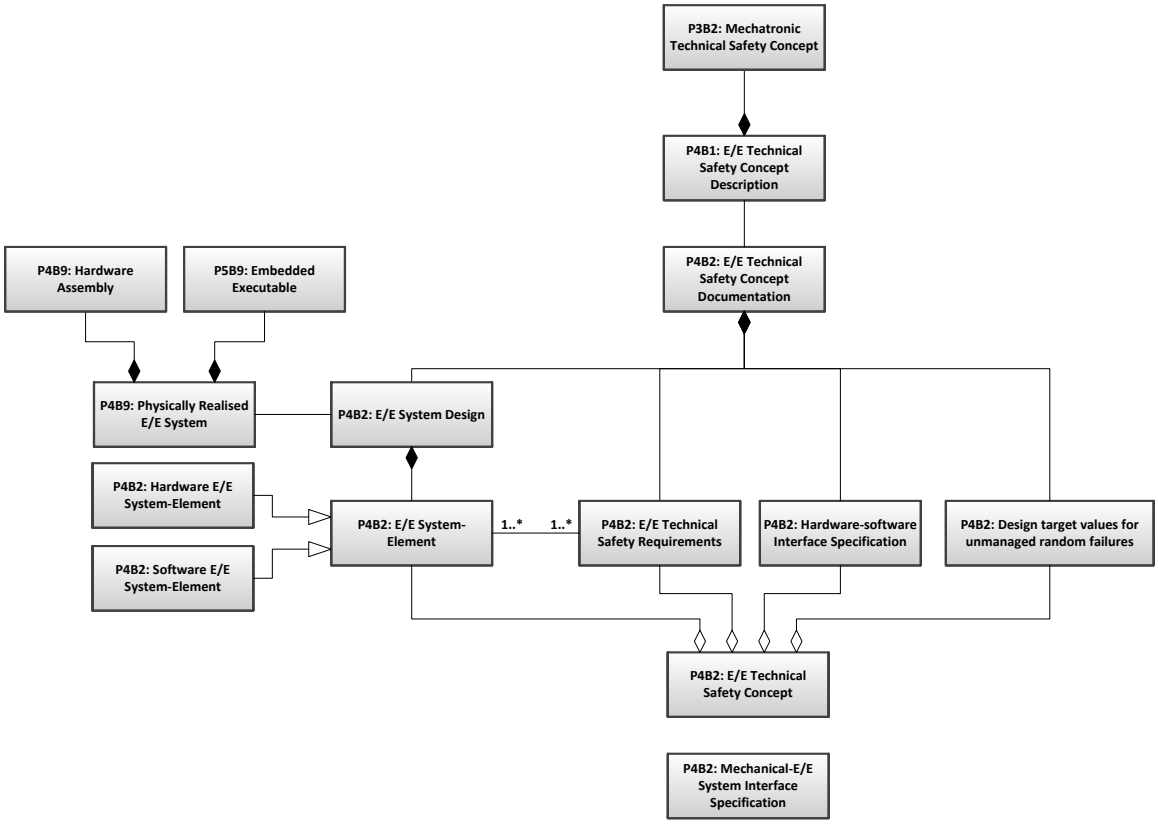

Figure 62: Pars 4 E/E System Technical Safety Concept - Pars Design Description, Pars Design and Pars Realisation

Mechatronic System Example	**E/E System Example**
P3B2: Mechatronic Technical Safety Concept	P2B2: Functional Safety Concept
P4B1: E/E Technical Safety Concept Description	P3B1: Technical Safety Concept Description
P4B2: E/E Technical Safety Concept Documentation	P3B2: Technical Safety Concept Documentation
P4B2: E/E System Design	P3B2: System Design
P4B2: E/E System-Element	P3B2: System-Element
P4B2: E/E Technical Safety Requirements	P3B2: Technical Safety Requirements
P4B2: E/E Technical Safety Concept	P3B2: Technical Safety Concept

Table 10: Renamed E/E System Example Technical Safety Concept Blocks

4CAS Example

The *4CAS E/E System Technical Safety Concept* is shown as a BDD in Figure 63. This shows the sensors and actuators now in the context of the external interfaces. The IBD shown in Figure 63 specifies the technical implementation of the interface between the *E/E system* and the mechanical components.

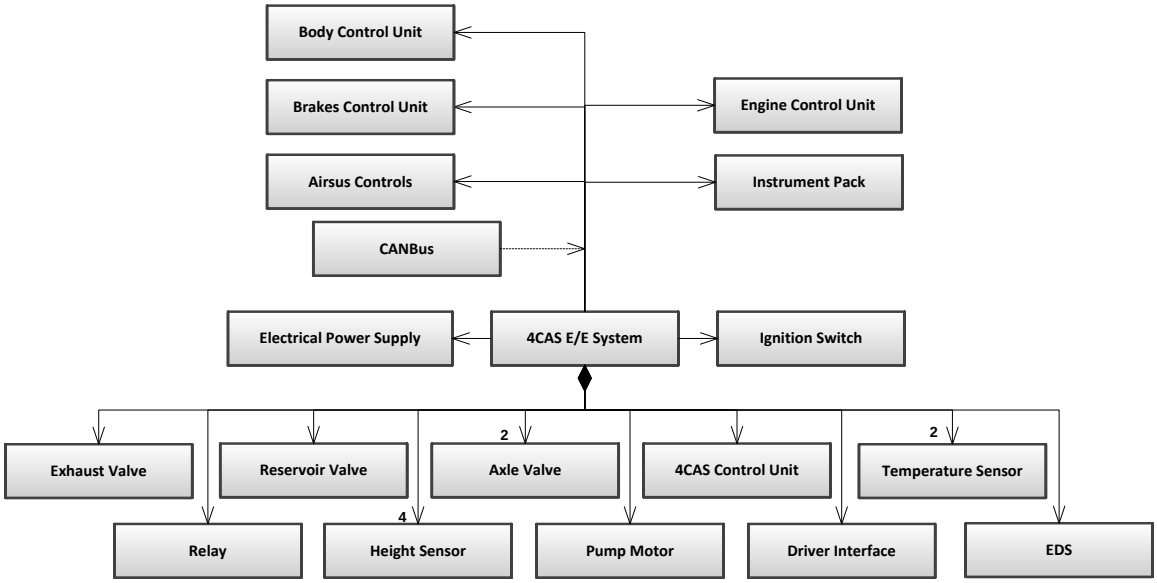

Figure 63: 4CAS E/E System Technical Safety Concept BDD

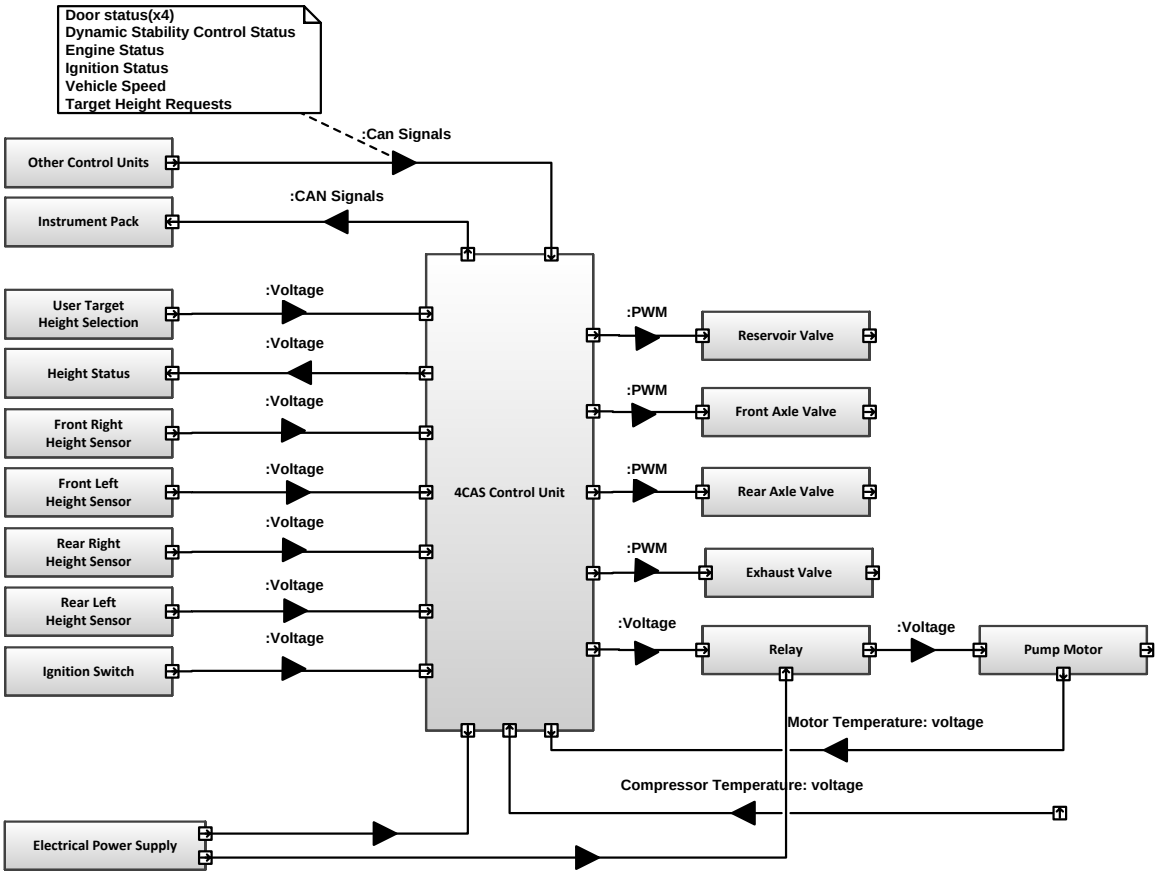

Figure 64: 4CAS E/E System Technical Safety Concept IBD

Safety Argument

The instantiation of the argument pattern is shown in Figure 65. It is identical to the *E/E system Pars 3 System Design including the Technical Safety Concept* except that terms have been renamed to match the mechatronic ontologies.

4.2.5 Pars 5 Hardware Design

This *Pars* is identical to the *E/E system* example except that *P3B2: Technical Safety Concept* is renamed to *P4B2: E/E Technical Safety Concept*.

4CAS example material is not presented.

4.2.6 Pars 6 Software Design

This *Pars* is identical to the *E/E system* example except that *P3B2: Technical Safety Concept* is renamed to *P4B2: E/E Technical Safety Concept*.

4CAS example material is not presented.

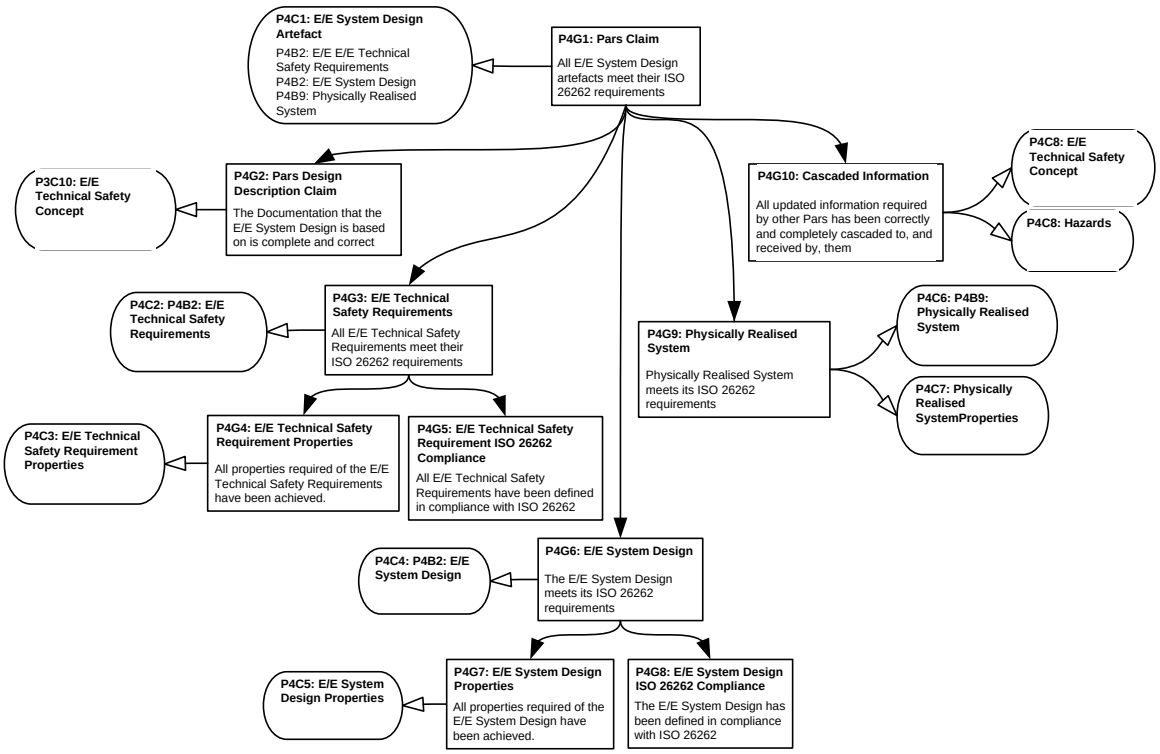

Figure 65: Pars 4 E/E System Safety Argument

4.2.7 Pars 7 Mechanical Design

The *Pars* 7 *Mechanical Design* diagram is shown in Figure 66.

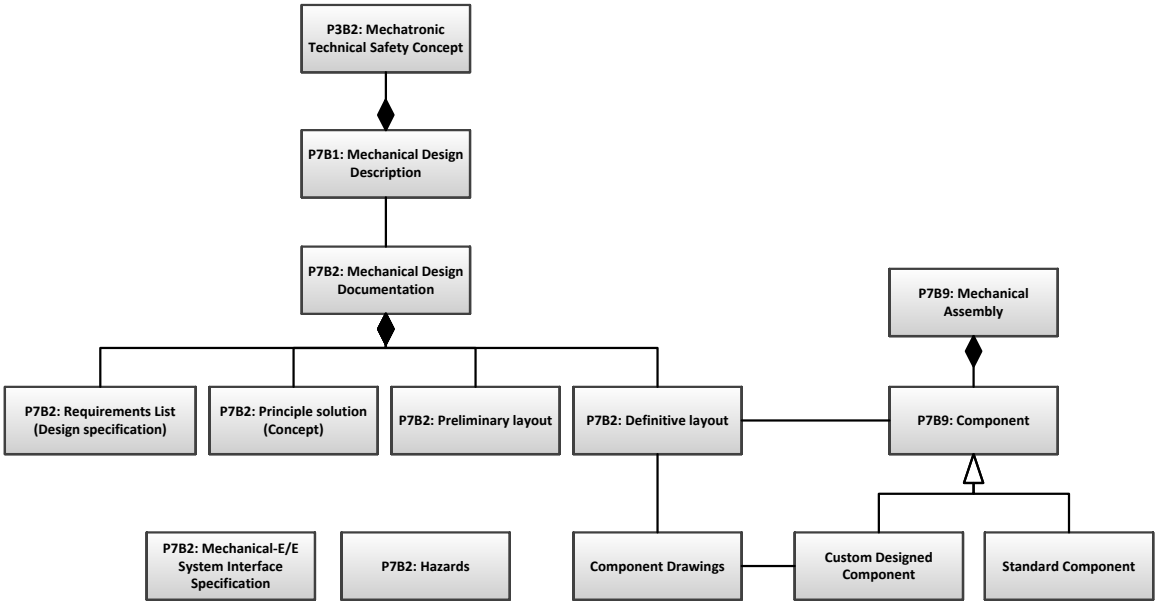

Figure 66: Pars 7 Mechanical Design - Design Description, Design & Realisation

Design and Physical Realisation

The *B1: Pars Design Description* is instantiated as *P3B1: Mechatronic Technical Safety Concept Description* and consists of *P2B2: Mechatronic Functional Safety Concept* cascaded from *Pars* 2. The *Mechatronic Functional Safety Concept* is composed of the *mechatronic system* architecture, the *Mechatronic Functional Safety Requirements* assigned to elements of the architecture, the *Mechanical-E/E System Interface Specification* and the rationale underpinning the safety concept.

The *B2: Pars Design* is instantiated based on a high level mechanical design process taken from Pahl and Beitz, [48], see Figure 9.

The model also shows instances of *B6: Aspect Cascaded to other Partes*. *P4B2: Mechanical-E/E System Interface Specification* represents the need for this specification to remain consistent with both *E/E system* design and *mechatronic system* design which necessitates a dialogue between the two *Partes*. In our model, changes to the document are cascaded to *Pars 3 Mechatronic the Technical Safety Concept*. *P7B2: Hazards* acknowledges that new hazards may be identified at any stage of the design process; they are most likely to be identified when establishing the properties of the design. Any hazards identified would be cascaded to *Pars 1 Mechatronic Item Definition and the Hazard Analysis and Risk Assessment*.

Properties

Given the high-level process view used to describe the design, it is not possible to define specific properties of the design artefacts as for the other *Partes*. The literature on mechanical design is not

described with the underlying model that we are using here. The literature indicates topics to be considered for mechanical components; one example is a checklist for embodiment design topics taken from Pahl and Beitz, [48], Table 11. Another example is a list for product evaluation topics taken from Ullman, [38], Table 12.

Topic	**Examples**
Function	Is the stipulated function fulfilled? What auxiliary functions are needed?
Working principle	Do the chosen working principles produce the desired effects and advantages? What disturbing factors may be expected?
Layout	Do the chosen overall layout, component shapes, materials and dimensions provide: adequate durability (strength) permissible deformation (stiffness) adequate stability freedom from resonance unimpeded expansion acceptable corrosion and wear with the stipulated service life and loads?
Safety	Have all the factors affecting then safety of the components, of the function, of the operation and of the environment been taken into account?
Ergonomics	Have the human-machine relationships been taken into account? Have unnecessary human stress or injurious factors been avoided? Has attention been paid to aesthetics?
Production Quality control	Can the necessary checks be applied during and after production or at any other required time, and have they been specified?
Assembly	Can all the internal and external assembly processes be performed simply and in the correct order?
Transport	Have the internal and external transport conditions and risks been examined and taken into account?
Operation	Have all the factors influencing the operation, such as noise, vibration, handling, etc. been considered?
Maintenance	Can maintenance, inspection and overhaul be easily performed and checked?
Recycling Costs	Can the product be reused or recycled?

Table 11: Embodiment Design Topics taken from Pahl and Beitz, [48]

Performance
Accuracy, variation, and noise
Tolerance
Sensitivity
Robustness
Manufacture
Assembly
Reliability
Maintenance
Environment

Table 12: Product Evaluation Topics taken from Ullman, [38]

These topics imply properties of the design artefacts, but they are not stated explicitly. Specific techniques for addressing the topics may reveal the underlying properties required, but the techniques are not given in the literature.

Testing is part of the mechanical design process, for example Ullman, [38] describes a five-step testing process to achieve robustness, based on Taguchi. In the argument this would be a property of one or more of the design artefacts.

If the mechanical design is carried out within a defined process this will mandate the creation of particular artefacts; it may also require defined properties of the work product to be established and state how these properties are established. No example of such a process has been discovered in the public realm.

Just based on cascade of requirements, a key physical realisation property of the mechanical assembly in the mechatronic context is that it is compliant and complete with regards to

Mechatronic Technical Safety Requirements assigned to it and to the *Mechanical-E/E System Interface Specification.* As mentioned previously, these properties could be established by the use of test techniques in a similar way as for the *E/E system.*

From the safety perspective, a key design property required of the mechanical design is that it is robust against the causes of systematic faults and the effects of systematic faults. To be consistent with the rest of the argument, this property would be established to an integrity commensurate with the rest of the development as indicated by the assessment of the unmitigated risk. As will mentioned in the discussion below, this is the prime property that we will consider in the remainder of the thesis.

4CAS Example

The primary aspect of the mechanical design from a *mechatronic system* perspective is the pneumatic system that directly interfaces to the electronic controller. The pneumatic system design is shown as a BDD in Figure 63 and an IBD in Figure 63. The details drawings behind these diagrams is outside the scope of this thesis.

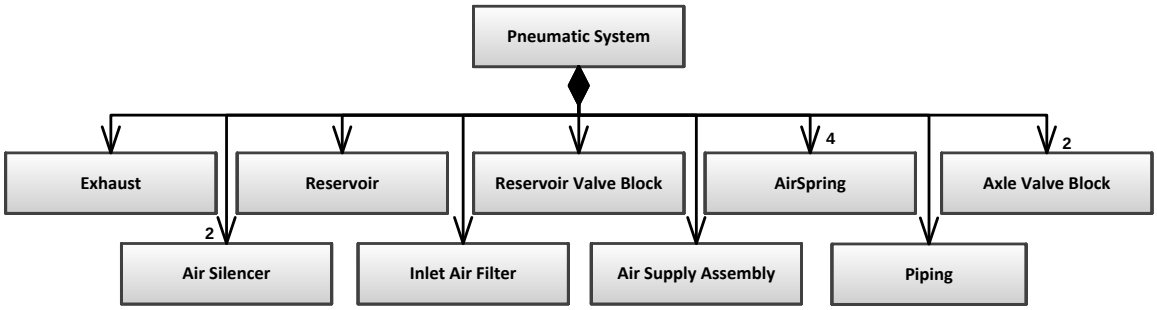

Figure 67: Pneumatic System BDD

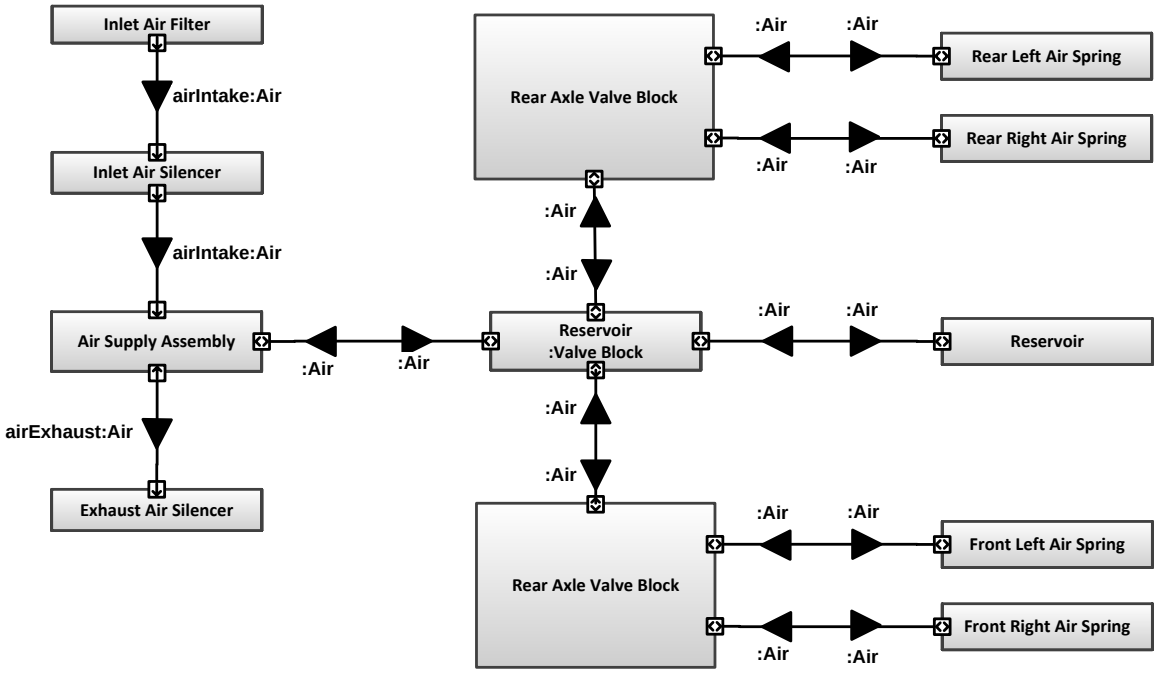

Figure 68: Pneumatic System IBD

Safety Argument

The instantiation of the argument pattern is shown in Figure 69. While there are standard parts of the argument that can be instantiated, the artefacts are taken from the ontology given in Figure 66. As this is a very generic ontology, no details about design artefact are known so the argument shows these in an equally generic manner. The realisation artefact has been shown separately

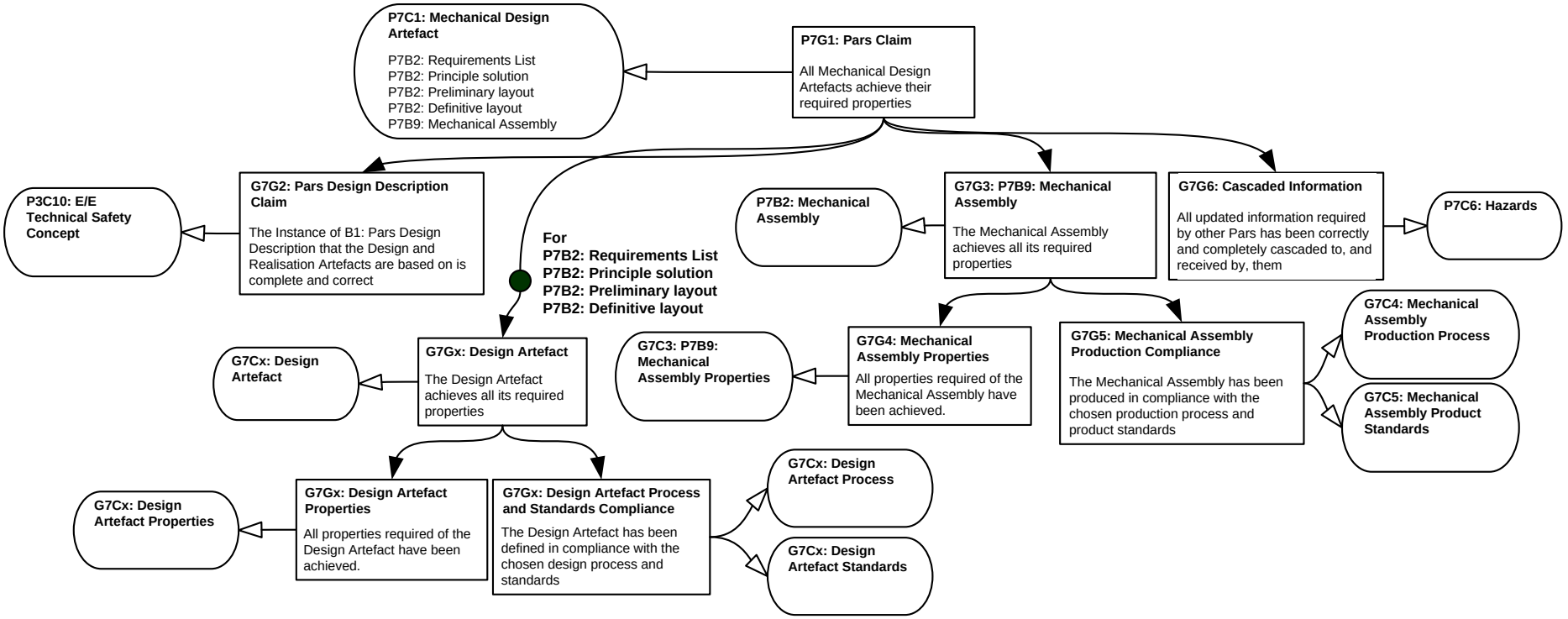

Figure 69: Pars 7 Mechanical System Safety Argument

4.3 Discussion

At this stage in the exposition of the *Pars* approach we have seen that it can be applied to a *mechatronic system*. The 4CAS illustration has given some impression of what the design material could look like in practice.

We have noted that hazards, which are a key factor in risk assessment, can be identified in different *Pars*, although the primary one is *Pars 1 Mechatronic Item Definition and the Hazard Analysis and Risk Assessment*. In practice, for the risk assessment of an *E/E system*, it has always been necessary to take into account the capabilities of the actuators and their potential effect on the mechanical components in order to assess severity and controllability. So, the *Pars 1* for a *mechatronic system* is not significantly different to the equivalent for an *E/E system*.

The *Pars* division adopted here has a *Pars* for *Mechatronic Technical Safety Concept* and another for *E/E Technical Safety Concept*. Another approach would be to a single *Mechatronic Technical Safety Concept Pars* which covers the whole of the *mechatronic system* design in terms of mechanical, hardware and software. The benefit of this approach is that when designing a *mechatronic system* it is necessary to consider the trade-offs between mechanical, hardware and software all at the same time. The current scheme was adopted as it is the closest approximation to the way the project was organised; in practice, the issue was handled by communication between the mechanical and E/E staff who also worked together on the *mechatronic system* design.

It was highlighted in section 0 that, from the safety perspective, a key design property required of the mechanical design is that it is robust against the causes of systematic faults and the effects of systematic faults. The question arises as to how this design property can be established for the mechanical design. It is proposed that the design FMEA process be used to achieve this. The proposal is made on the basis that, in the automotive industry, the technique has universal use at the component level and is also widely used at the system level. There are two issues that arise with this proposal.

The first issue is that to be consistent with the rest of the argument, the property would have to be established to an integrity commensurate with the rest of the development as indicated by the assessment of the unmitigated risk. For the *E/E system* this is achieved by the assignment of an ASIL value to the safety requirements and then the ISO 26262 standard providing the guidance on how to achieve the specified integrity. A value of ASIL cannot be assigned to safety requirements placed on the mechanical elements of the architecture, so this begs the question of how the concept of design integrity can be fed into the mechanical design process. Here we note the problem and address it in Chapter 6.

The second issue is whether the practical use of the design FMEA does, or has the potential to, provide the evidence we require to establish the property of robustness against the causes of systematic faults and the effects of systematic faults. To investigate this further a case study was conducted to address the question: *What is the established role and practice of using FMEA in an automotive context and the factors that influence its judged effectiveness?* In Chapter 5 we describe the case study and report the results.

4.4 Summary

We have shown that the *design model* can be applied to a *mechatronic system* and that the elements of the model can be mapped to design artefacts that are typically available in a practical development. We have also shown how safety argument structure from Chapter 3 can be recast for a *mechatronic system*. An example instantiation of safety argument for a *mechatronic system*, using the 4CAS system, is given in Appendix C.

We have highlighted the issue of bringing the concept of *integrity* into the mechanical design and will address this in Chapter 6.

We have also highlighted the need to understand the potential of the FMEA, as performed on mechanical components, to provide supporting evidence for the safety argument. This is addressed in Chapter 5.

Chapter 5 DFMEA Usage Case Study

5.1 Introduction

In Chapter 4 we saw the need to investigate whether the practical use of the design FMEA, (DFMEA), as performed on mechanical components, has the potential to provide the evidence to support the *mechatronic safety argument*. While we have seen that the safety argument can be recast for a *mechatronic system* this will be to no avail if there is no means of providing the necessary evidential support from the mechanical design. Ideally we would like evidence to support the MISRA, [187], claim types of *rationale*, *satisfaction*, *means* and *organisational environmen*t. In this chapter we report the results of a case study into the practical use of the design DFMEA.

An introduction to the FMEA technique was given in Chapter 2, 2.3.3, and fuller exposition is given in Appendix A. In the automotive industry, failures of mechanical components are managed by a quality process that uses the Failure Mode Effects Analysis (FMEA) technique, [159]. FMEA is an analysis technique that determines failures and their causes and mitigates their causes or effects by specifying control measures; these include product requirements and test procedures, [170], [171]. We also saw in section 2.3.3 that the use of DFMEA is central to a number of different quality processes, e.g. robustness, failure mode avoidance. These primary address quality in terms of warranty and customer dissatisfaction. It is only for a minority of systems that are historically seen as being safety related, e.g. brakes steering. This makes the DFMEA a prime candidate for the source of the evidence necessary to extend the safety argument to the identification and mitigation of malfunctioning behaviour caused by the failures of mechanical components. However, at present the processes supporting compliance with ISO 26262, [13] are quite distinct from the DFMEA-based quality processes, despite the fact that software control is often used to achieve the required performance of a mechanical component.

To understand the extent to which the DFMEA, as practised, does, or could, produce the evidence necessary to support the argument pattern described above, a qualitative case study has been performed and reported in this thesis, to address the following research question:

What is the established role and practice of using DFMEA in an automotive context and the factors that influence its judged effectiveness?

In this study, the DFMEA had been applied to mainly mechanical components. Semi-structured interviews were used as the primary data collection instrument in this research. General questions were asked to get an understanding of what practitioners thought they were doing and why; these were based on a documented DFMEA-based quality process. Here, quality is used as an umbrella term that covers the absence of all negative customer experiences associated with the component. The questions were aimed at understanding if the results of the DFMEA could serve as evidence

for the safety argument. We were also interested to understand if the use of the DFMEA would benefit from it having an assurance case structure.

It is not feasible to assess the whole of the automotive industry, therefore, the scope of the case study has been restricted to a single company which is a major global automotive OEM whose approach is representative of the industry in general. This approach produces depth rather than breadth of analysis.

The FMEA technique can be applied to different aspects of the engineering process, for example to a concept, a design or a process. However, in this thesis, unless otherwise stated, the term DFMEA is used in the context of application to a design, although the distinction between a concept and a design is often a moot point. Failure Modes Effects Criticality Analysis (FMECA) is also a term in common usage; in this thesis the term DFMEA is used as it is the one in most commonly used, but it does include the criticality analysis, [193].

5.2 Background to Case Study

This section describes the design of the case study and the data collection method. The company in which the case study was conducted has a documented DFMEA process, [194], based on SAE J1739, [159]. As mentioned above, semi-structured interviews were used as the primary data collection instrument in this research. In order to answer the research question, it is necessary capture the views of those who are responsible for performing and reviewing DFMEA. The data to be captured is not quantitative and so a qualitative technique, such as semi-structured interviews, is appropriate.

5.2.1 Case Study Design

The case study looked at how the DFMEA technique is used across the whole of a single company. The structure of the case study is based on Yin's Case Study Research methodology [195]. According to Yin's classification, the proposed study is a Type 2: Single-case embedded design. It is a single-case design because it is capturing *"... the circumstances and conditions of an everyday situation*". It is an embedded design because there are multiple units of analysis; in this case each person interviewed is a different unit of analysis.

Following Yin, the preparatory work included creating an initial *theory* to help define the research propositions and evaluation criteria used in the case study. The relationships between the key terms of interest, taken from the standards, literature and the author's previous training and experience, were captured in a diagram, Figure 70. The lines between the terms represent the relationships as understood before the case study was performed. Those terms considered relevant to understanding the traditional use of DFMEA in the context of functional safety are highlighted.

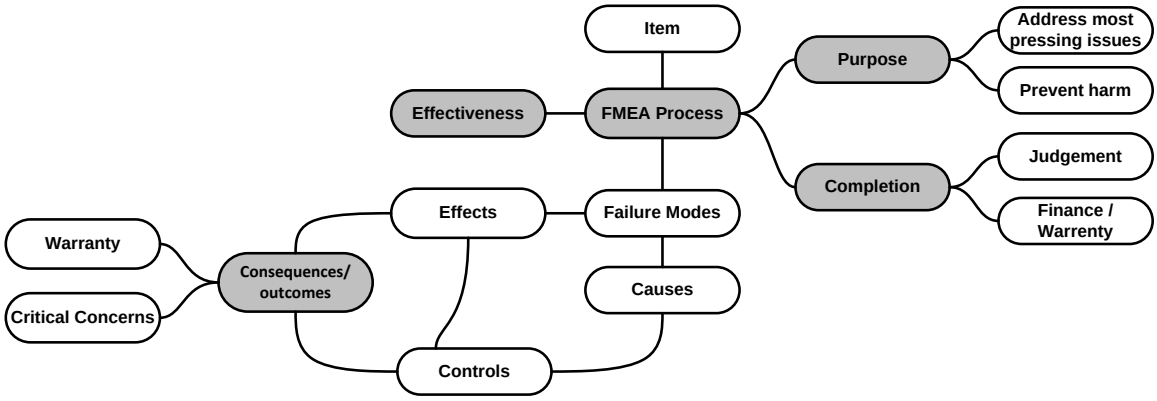

Figure 70: Initial Theory

It was assumed that the purpose could be summarised as addressing the most pressing issues, which may include harm to people. However, the issue of harm was investigated in particular as functional safety is exclusively concerned with harm. How staff consider the process to be complete is of interest, as ISO 26262 has strong completion criteria based on the production and content of a defined set of work products. The constraints on effectiveness were investigated to understand to what extent they are inherent and to what extent they are dependent on the application of the process. The DFMEA process was investigated to discover how staff understood the relationship between failure modes, causes, effects and controls; these types of relationships are defined in detail in ISO 26262. The outcomes of not performing the process effectively is of interest as this is a possible link to functional safety; it was assumed that warranty and critical concerns would be the main considerations.

Although the research question is based around role, factors and practice, the questions were structured around the company procedure as this was the document that all the participants were familiar with. A mixture of open and closed questions were used. The closed questions were structured around a statement with degrees of consent. The open questions were more likely to elicit what the participant really thought, but were harder to process. The questions are shown in Appendix D. Questions numbered 2.x concern the philosophy of DFMEA and are intended to elicit the participant's understanding of the purpose and rationale behind the DFMEA technique. Questions numbered 3.x concern the practice of DFMEA and are intended to elicit what the participant actually does.

As mentioned above, the unit of analysis is the individual participant and a total of 16 participants were interviewed. The first participants were identified by virtue of them having prominent roles in the organisation; further participants were identified by asking for suggestions as part of the case study (*question 3.18 Is there anyone else that you think I should talk to?*). The full complement of participants was chosen so as to have a spread of different roles within different departments, as shown in Table 13 and Table 14. The final set of participants is a good and representative sample because it includes staff from departments across the company and includes both practitioners, who

perform DFMEAs as just one task in the development of their component, and also experts who use the technique on a daily basis.

The study had the ethics approval from Physical Sciences Ethics Committee at the University of York.

Quality Engineer	7
Six Sigma Master Black Belt	5
Engineer	3
Quality Manager	1

Table 13: Participant by role

Body	5
Powertrain	5
Chassis	2
Electrical	2
Research	1
Quality	1

Table 14: Participant by department

5.2.2 Data collection

The interviews were conducted over a six- month period starting in February 2015 with the last one conducted in July 2015. Each person was interviewed separately and the interview lasted about one hour. The answers given were recorded by hand on a hardcopy of the questionnaire template. If the participant made side remarks or gave other information not directly related to the question, this was recorded on a separate piece of paper. The results of each interview were transferred to electronic media, i.e. a spreadsheet, within 48 hours of the interview. When transferring the results, errors in grammar and punctuation in the handwritten notes were corrected.

5.2.3 Data Analysis

The open questions were intended to provoke comments; some participants only gave minimal answers while others made comments even when answering closed questions. All the comments from all participants were listed; where a comment made several points, each point was listed as a separate comment. The questions that produced comments and the number of comments associated with each question, 165 in total, are shown in Table 15.

Questions	Q2.9	Q2.8	Q2.11	Q3.13	Q2.5	Q3.17	Q2.1	Q2.12	Q3.9	Q3.11	Q2.3	Q2.10
Comments	36	30	24	24	16	9	8	7	7	2	1	1

Table 15: Comments versus Questions

The comments were processed using the principles of thematic analysis, [196]. First, they were grouped under the research subject matter topics of role, practice and factors. The grouping was based on the content of the comment with most comments clearly falling into just one of the topics. Where this was not the case, then the comment was included in the grouping of more than one topic. Within each topic group the comments were grouped further as themes. Some themes were inherent

in the original construction of the questionnaire while others were identified on the basis of the number of times the subject was mentioned or the number of closely-related comments. For example, many comments were made about the characteristics of a well- performed DFMEA, see below. The results are presented in the next section under the headings of role, practice, effort expended and factors.

5.3 Case Study Results

5.3.1 Role

The participants were directly asked what they thought the purpose of the DFMEA was, question Q2.1, and the author's preconceived idea was explored in question Q2.2. Their view on the use of the DFMEA as a means to avoid harm was explored in question Q2.3. In response to questions Q2.2 and Q2.3, all but one of the participants either *Agreed* or *Strongly Agreed* that the purpose of a DFMEA included *improving the component being analysed by addressing its most pressing issues and preventing the product from causing harm*. One participant *Disagreed* with the statement in question Q2.3 on the basis that with most systems it is difficult to change the effect and so the potential for harm cannot be avoided, therefore the focus is on addressing the cause. Comments made when answering other questions also revealed the participant's view of the role of the DFMEA; the main themes are shown in Table 16.

Id	Purpose
1	Prevent failures by identifying the necessary controls
2	Assess risk of failure
3	Identify failure modes
4	Understand the design better and record this understanding
5	Provide a systematic analysis process as part of systems engineering

Table 16: Purpose of Performing an DFMEA

The majority of the participants highlighted the role of the DFMEA in identifying *controls* which minimise the occurrence, or maximise the detection, of failure modes and their causes. *Controls* related to testing were mentioned most often. Several participants also mentioned updating internal design standards and internal test procedures based on lessons learnt from previous experience, as represented by item 4.

In mentioning *Risk*, Id 2, participants were indicating that understanding the *risk* associated with the failure modes was a key aspect of the process and that the *risk* determined the priority given to putting controls in place to *prevent failure modes escaping*. This is supported by the response to question Q2.2, where all participants *Agreed* or *Strongly Agreed* that one purpose of a DFMEA is to improve the component being analysed by addressing its most pressing issues. *Risk* in this context refers predominantly to negative effects relating to customer satisfaction and experience, survey results, warranty figures and recalls. However, of the 16 participants, 15 *Agreed* or *Strongly Agreed* that one purpose of a DFMEA is to prevent the product from causing harm, where, in the context

of this question, harm does refer to physical injury to people. This is reinforced by the response to question Q2.6 where 15 out of 16 agreed that performing an DFMEA could avoid Critical Concerns; these are issues experienced in the field with a potential to cause harm. The dissenting participant took the harm to be a consequence of the effect and reasoned that to prevent harm it is necessary to have a different effect; the effect is inherent in the design being analysed, so performing a DFMEA will not change this. They saw the focus of the DFMEA to be on prevention by addressing the cause. This is in effect the same understanding as the other 15 participants. All but two of the participants *Agreed* or *Strongly Agreed* that the concept of risk associated with the product causing harm to someone is common across all engineering disciplines. The other two participants took the question to refer to the commonality of severity across different vehicle components and responded that different components have different failure modes with different severities.

In mentioning Design, Id 4, participants were highlighting the role that the DFMEA plays in developing a robust design that is free from what would otherwise be overlooked failure modes, Id 3. The fact that the DFMEA process is systematic, Id 5, and could be used to record the design rationale and capture the previous experience, Id 4, was also appreciated. Mention was also made of the role of the DFMEA in delivering customer satisfaction and documenting requirements.

The most common term used to refer to issues relating to the product injuring people, Q2.4, was severity. In response to question Q2.13, all but two of the participants *Agreed* or *Strongly Agreed* that the concept of risk associated with the product causing harm to someone is common across all engineering disciplines. This was based on the fact that a common scoring system is used for all components and that the customer experience at the vehicle level is independent of the underlying technologies. Some participants observed that the common scoring system has some difficulties in that the severity ranges from irritation to serious injury and questioned whether such a single scale was appropriate. Some participants took the view that DFMEA only considered business risk and only defined outcomes in engineering terms.

5.3.2 Practice

The actual practice of the DFMEA authors and reviewers is presented in this section. It is largely based on the structure of the survey questions, but some of the responses to the open questions produced answers that can be taken as characteristics of a well-performed DFMEA.

Characteristics of a well-performed DFMEA

Combining answers from a number of questions, Table 17 presents the characteristics of what the participants consider to be a well-performed DFMEA.

There is evidence of stakeholder engagement
Everything based around functions with a good functional breakdown in a logical sequence
Functions are related to customer requirements
Function definitions are specific to the component and defined in scientific or engineering terms
All different types of failure modes are analysed
Many causes for each failure mode are considered
The causes are in the scope of the analysis
There are not an excessive number of low scores
Appropriate standards are specified as controls for each line of analysis
Prevention controls are linked to the design requirements specification
Test standards specified as controls represent a coherent series
Is consistent and has the appropriate level of detail that documents the thinking behind the product development
Does not have gaps and is not too repetitious

Table 17: Characteristics of a well performed DFMEA

Completion criteria

The participants were asked directly, Q2.5, what completion criteria they used and, in particular, the extent to which completion of the analysis is based on judgement or on financial considerations, e.g. the warranty costs. 13 of the participants *Agreed* or *Strongly Agreed* that completion was a judgement made by the leader, or the whole team, based on their experience. The participants were split, 10 (Disagree) and 7 (Agree), on whether financial considerations were taken into account when making the judgement. Those who disagreed mentioned the use of DFMEA assessment criteria; see *Judgement of quality* in section 5.3.4. A number of other criteria were also mentioned, see Table 18.

Check that all the correct controls are in place and actioned
Check that the risk assessment scores cannot be reduced more, particularly high severity scores
Check the analysis has been performed to the appropriate depth
Perform a system review
Take programme timing into account

Table 18: Completion Criteria

Causal analysis

One step of the DFMEA it to determine the cause of the failure. There is a hierarchy of causes starting from the failure, and the level at which the analysis stops is to a degree arbitrary. The company guidelines acknowledge a *first level cause* and a *root cause*. The determination of the cause can be performed informally, as a mental exercise; there are also more formal techniques, referred to as *root cause analysis*. Typical *root cause analysis* techniques used are the 8-D process, [197], and applying the 5-Whys method, [198], to an Ishikawa Diagram, [140]. The 5-Whys technique may be performed in the meeting but not formally documented. The participants were asked directly, Q3.12, how often they performed this analysis. The results, Figure 71, show that there was a wide range of responses; this is due to the different roles of the participants. In *normal* product development it is not used often, whereas for trouble-shooting it is often used.

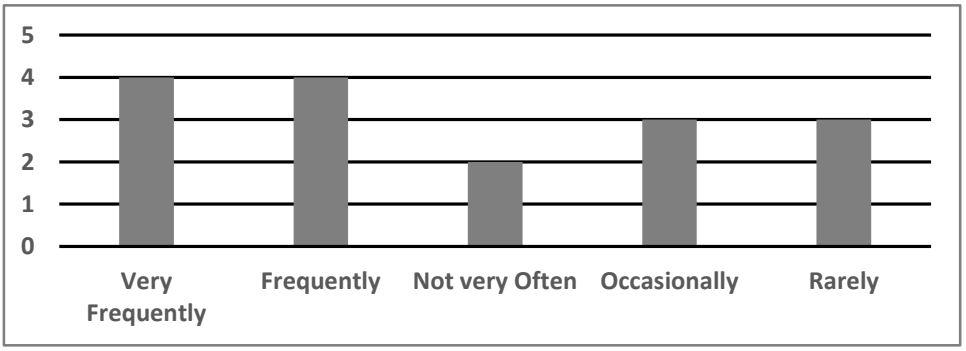

Figure 71: Use of Root Cause Analysis

The participants were asked, Q2.12, what factors they take into consideration when deciding to perform *root cause analysis*. For a new development, participants take into account known bad experiences from previous vehicle programs, while drawing a balance between analysing everything and working within set timescales. They also take account of the severity and occurrence rankings. For a production item that is exhibiting a problem, the decision to use *root cause analysis* is based on the magnitude of the problem as judged by the warranty costs being incurred, the level of customer dissatisfaction and any white alerts. *Root cause analysis* may also be used in response to an official problem report raised against a component. Some participants also said that the decision to perform *root cause analysis* is influenced by the analysis itself. For example, it is more likely to be performed if the noise factors are not understood or if three or four different noise factors affect the same function. It is also used when it is not obvious what controls should be specified, because the current identified cause is not at a level that can be acted upon.

The participants were asked, Q3.13, what they considered the most common *root causes* to be. The answers related to either the process, Table 19 or the product, Table 20. Those topics given as *process root causes* lead to the *product root causes*.

	Design	**Manufacturing**
Poorly performed DFMEA	y	
Staff not given the necessary training	y	
Occurrence of design errors across boundaries of responsibilities	y	
Incorrect original requirement	y	
Incorrect understanding of how related parts function	y	
Incorrect or undefined interfaces	y	
Poor or missing standards	y	
Poor requirement cascade	y	
Poor communication between design and manufacturing	y	
Analysis not revised when changes to the component made	y	
Batch errors		y
Incorrect part has been fitted		y
Incorrect process has been used		y

Table 19: Common Process Root Causes

Effect due to extremes of the 5 noise categories
System level/component level interactions
Use of the wrong material
Use of the wrong material for a given market
Bulk failures
Unsuitable surface finishes
Unanticipated load or torque values
Tolerance stacks
Environmental effects

Table 20: Common Product Root Causes

5.3.3 Effort expended

The participants were asked directly, Q2.14, whether the effort they expended on understanding risk, mitigating risk and gaining confidence in risk mitigation depended on the magnitude of the risk or the criticality of the product failure. All but two of the participants *Agreed* or *Strongly Agreed* that this was the case. The general consensus conformed to the view of one participant that there is a descending hierarchy of risk, e.g. injury, legal, fit/finish and customer irritation, with more attention being given to issues the higher up the hierarchy they were. However, one participant, while acknowledging this, suggested that it was not necessarily the right approach as the customer is still inconvenienced, even by low-severity issues. There was agreement that effects given a YC classification, see section 4.3.2, have the top priority; this was reinforced by the perception that the DFMEA is a legal document and so there is legal liability if higher risks were not dealt with properly.

One participant *Disagreed*, on the basis that lower severity effects are more common and cause the majority of the customer complaints, so they are addressed with the same effort as high severity affects. Another participant *Strongly Disagreed*, believing that severity only influences effort if a high severity event occurs in the field. One can see from these that in the minds of the participants, risk is often equated to severity.

***Scoring*[2]**

The assignment of an Occurrence Ranking Number and a Detection Ranking Number were addressed in questions Q3.2 and Q3.3 (*On what basis do you decide the prevention/occurrence score of an effect?*). The author made a mistake when preparing the questions; the occurrence score is an assessment of the effectiveness of the prevention design control and there is no separate score for prevention; this error was pointed out by many of the participants. Question Q3.2 should have been about the Detection Ranking Number. For the purposes of this analysis the answers for Q3.2 and Q3.3 have been combined as occurrence and shown in Figure 72.

[2] While the standards use the term *ranking* for assessing severity, detection and prevention, the company procedure uses the term *score*.

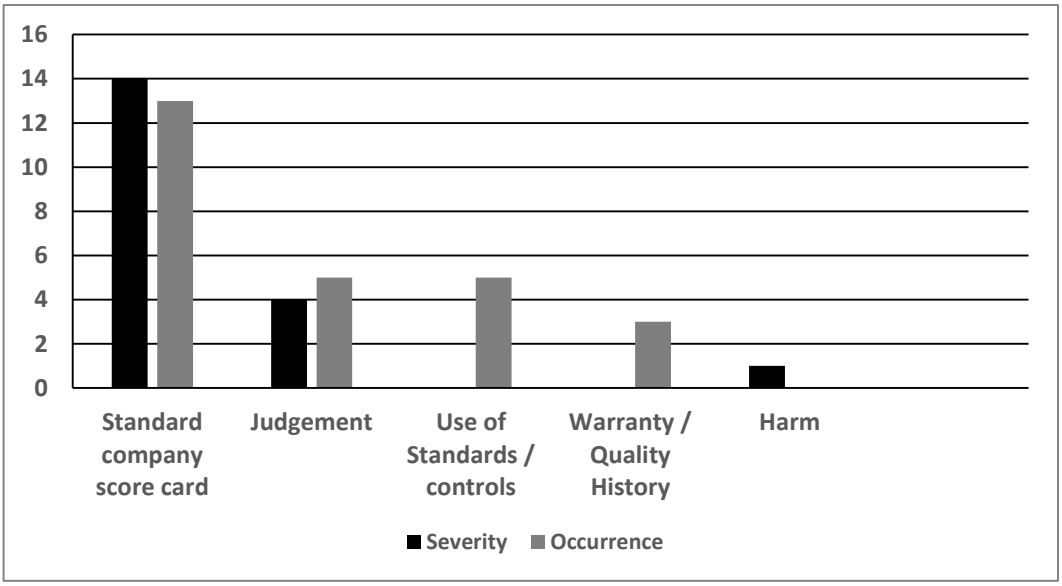

Figure 72: Q3.2, Q3.3 Basis of Severity and Occurrence Scores

The most common basis for the assessments is the standard company score guideline followed by judgement. The use of standards and other controls is a significant factor along with feedback from the field in the form of warranty or general quality history. It is unlikely that the mistake in formulating question Q3.2 has made a significant difference to the answers given. In practice, all the Ranking Number assignments, including those for severity, are judgements and many participants acknowledged this. This does not mean that those who did not make this comment did not understand that this was the case. The answers to questions Q3.9 and Q3.10 concerning the adequacy of design controls show that judgement plays the largest part, with only a few mentions of simulation and test representing something more objective.

Significance of a YC Classification

The company guidelines deprecate the use of RPN and prefer the use of a Severity Classification (YC), a Severity/Occurrence classification (YS) and a Detection Ranking criterion. A failure mode with a Severity Ranking Number of 9 or 10 is designated as a *YC* on the basis that it affects safe vehicle or product function and/or compliance with government regulations. A failure mode with a Severity Ranking Number between 5 and 10 associated with a cause that has an Occurrence Ranking Number of less than 3 is designated a *YS* if it has not already been designated as a *YC*. The guidelines require that each line of analysis in the DFMEA with a YC or YS designation has an action associated with it. An action may relate to a design change, the use of Prevention or Detection Design Controls, or the need to alert others to particular issues e.g. manufacturing, assembly, supplier, shipping. If neither designation has been assigned, an action is also required if the line has a Detection Ranking Number greater than 3. The interviews only investigated the use of the YC classification because this may relate to issues considered safety related and so was relevant to the case study. The relevant questions are Q3.4, Q3.5, Q3.6, Q3.7 and Q3.11.

Most participants agreed that the nature of an effect is an inherent property of the item being analysed because it was the working principle being exploited in the design, e.g. a hose containing fluid under pressure will always have being blown off as a potential failure mode. So only rarely could an effect labelled YC be designed out, and there was common agreement that in the majority of cases an effect labelled YC had to be mitigated by the use of controls.

There was some indication that effects labelled YC are given the highest priority, with two participants explicitly stating that those effects with a YC designation were the top priority. This included greater scrutiny of both Prevention and Detection controls to ensure effectiveness, with perhaps a greater emphasis on the Detection controls, and more involvement of senior management. Following industry practice as a guide for what can be accepted was also mentioned.

However, although effects labelled as YC are notionally more important than those not so labelled, in practice all effects are treated very similarly. This is because the effects that cause the majority of customer complaints and warranty returns are not labelled YC, and it is these issues that the DFMEA is used to address. Hence, most controls are associated with effects not labelled YC. One participant, commenting on the Occurrence Ranking Number, said that the score may be increased in order to produce a YC categorisation so that a control can be cascaded to the supplier or manufacturing. This is supported by the fact that most participants were of the view that deciding the sufficiency of the controls was unaffected by whether or not the effect had been given a YC designation, question Q3.11.

Failure Modes

The company guidelines advised the use of the five standard types of potential failure modes (*No Function, Partial – Over/Under Function, Degraded Over Time, Intermittent Function, Unintended Function*). All were considered equally appropriate and, of these, *Intermittent Function* and *Unintended Function* were generally considered to be the most difficult to assess, Figure 73. One participant commented that *Degraded Over Time* and *Intermittent Function* are really just the other types of failure mode arising in different circumstances. This practice is in line with the standards.

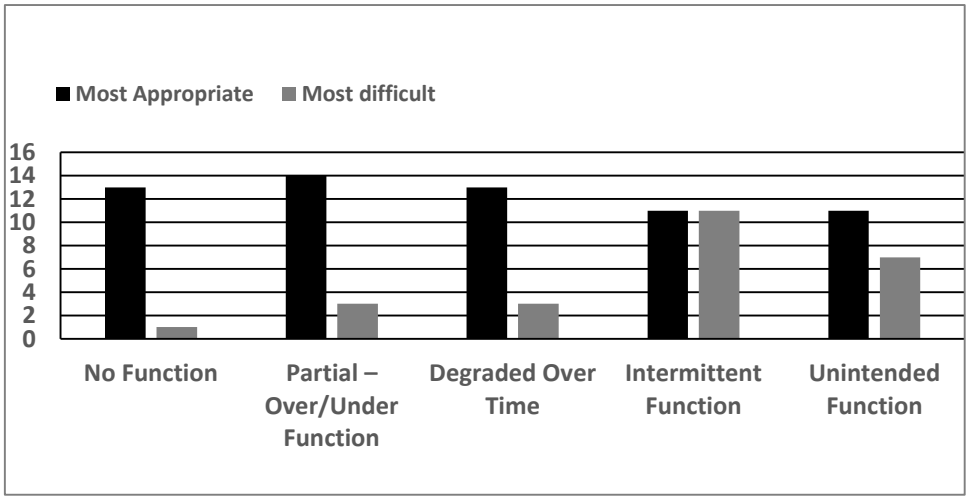

Figure 73: Use of standard failure mode types

Countermeasure sufficiency

The participants were asked directly, Q3.9 and Q3.10, how they decided that sufficient *Design Prevention* and *Detection Controls* had been specified. One participant commented that question Q3.9 was badly formed because countermeasures are linked to occurrence, not severity. Again, Q3.10 should have said *Occurrence* rather than *Prevention*. Despite these errors in the questions, the majority of participants answered the questions and a number of factors were mentioned, see Table 21.

Previous in-service experience of a similar product
The existence and quality of the standards specified as controls
The evaluation of the design to assess the effectiveness of the controls, e.g. by review, simulation, test
The consensus of the team based on their previous experience
The coverage of causes by controls
The nature of effect, e.g. injury, legal, degree of customer dissatisfaction
Reassessment of Occurrence Ranking in light of specified Prevention Control
The degree to which the functions and use cases have been covered

Table 21: Factors considered when deciding if sufficient controls have been specified

When and why are DFMEA reviews held?

Question Q3.14 was related to DFMEA reviews. Existing components have a foundation DFMEA which is used as a record of the learning from previous work on the component. These foundation DFMEAs are reviewed yearly, or on a rolling basis, so that a review is completed every 12 months. The purpose of the review is to check that all the previously identified issues have been addressed and that the DFMEA is up-to-date with the latest design. A DFMEA review is also performed for the deployment or further development of a component on a vehicle programme. Performing a DFMEA is part of the development process; the DFMEA is reviewed at the start of the development and then prior to each programme gateway to ensure that the DFMEA is complete and that the controls are in place and avoid late design changes. The last review ensures that the launch issues have been captured. A number of participants mentioned problems with modified components that

they attributed to a review of the DFMEA not being performed. The failure to review supplier DFMEAs was also mentioned as a source of some issues.

5.3.4 Factors

From the answers to the open questions it has been possible to get some insight into what factors are taken into account by the authors and reviewers of DFMEAs. The factors are presented as: outcomes to be avoided which affect the effort and judgement of completion, factors that hamper the process and have to be worked around, and how people consciously decide the quality of the DFMEA.

Outcomes to be avoided

The participants were asked directly, Q2.6, what would be the outcome if the DFMEA was not performed properly, with the suggestion that higher warranty figures and more critical concerns would result. All but one participant *Agreed* or *Strongly Agreed* that this would be the case. When asked what other negative outcomes may arise, a large number of issues were mentioned which can be grouped as *pre-production indicators*, Table 22, and *post-production indicators*, Table 23. The post-production issues can be further categorised as affecting cost, legal obligations or reputation, with anything that the customer is aware of having an adverse effect on the reputation of the brand.

More manufacturing and launch issues
Poor specifications and design
More late change resulting in longer development times
Increased cost
More problems with systems interaction

Table 22: Pre-production issues

	Cost	**Legal**	**Reputation**
Increased warranty costs	y		y
Ongoing issues			y
White Alerts and Recalls		y	
Customer dissatisfaction			y
More service issues	y		y
Poor results in external Surveys			y
Non-compliance with regulations		y	

Table 23: Post-production issues

Factors that hamper the DFMEA Process

The participants were asked how effective the DFMEA was in practice at achieving its purpose, Q2.7, and how often something is missed which should have been found, Q2.10. The answers to these questions are shown in Figure 74 and Figure 75.

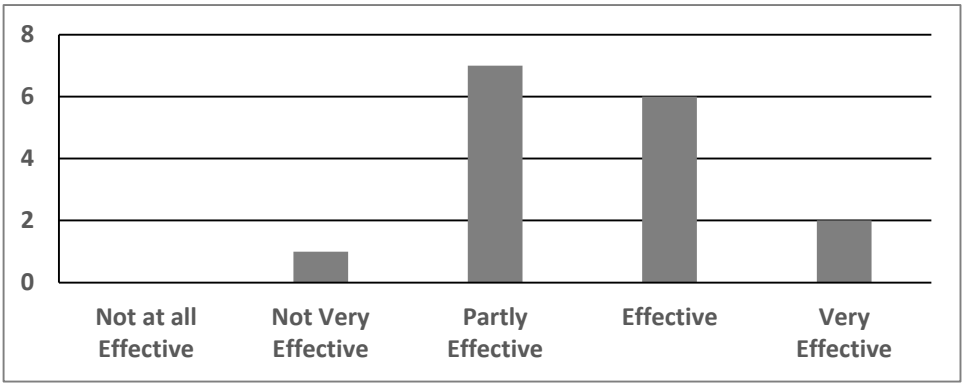

Figure 74: DFMEA effectiveness

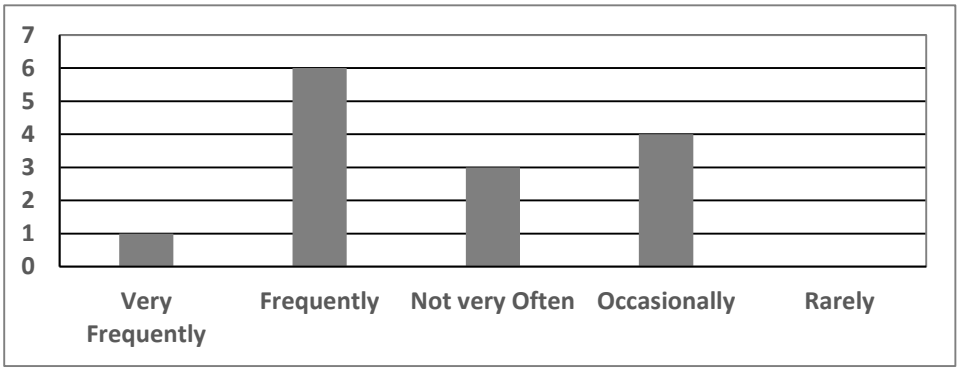

Figure 75: How often the DFMEA fails to find an issue

Although Figure 74 shows that the majority of participants consider the DFMEA to be effective, many caveated their response by saying that it had the potential to be effective but was let down by a number of factors; this is why Figure 75 shows that participants were also aware that issues were missed. A number of factors were mentioned to explain why issues were missed as shown in Table 24. These are discussed below.

Team and organisational issues
Failure to consider all relevant factors
Interface issues and complexity
Lack of resources
Lack of feedback
Lack of customer perspective
Level of detail
Misapplication
Not reviewing supplier's DFMEAs

Table 24: Factors hampering the potential effectiveness of the DFMEA

Unsurprisingly, a number of participants commented that effectiveness of performing a DFMEA depended to a large extent on the team, their knowledge and skills, also their motivation, thoroughness and willingness to put the effort in. A deficiency in knowledge and skills could be due to not having all the knowledgeable stakeholders represented in the team, or the team members not having sufficient training. In terms of team member's skill or creativity, one participant observed that engineers tend not to be good at thinking of possible failure modes but better at thinking of mitigations once the failure modes have occurred. It was thought that team members

may lack motivation because they were not aware of the purpose and potential benefits of performing a DFMEA. Often, team members believed that there is nothing left for the DFMEA to find because it was performed later than it should be and the engineers believed that failure modes had already been taken into account informally when performing the design activity. One participant summed it up as a cultural problem. The involvement of senior staff in reviews was thought to help counterbalance a tendency for the team to perform poorly and it also helps improve the culture. Effectiveness of the team was seen as being dependent on good relationships between team members; personality clashes were mentioned as being particularly detrimental.

Participants commented on the problems caused by responsibilities being split across internal and external organisational boundaries, which led to failures in communicating actions to others and in ensuring that the actions are carried out. As an example, the DFMEA process requires that manufacturing be informed that the DFMEA for a particular component had identified critical or significant characteristics (YCs or YSs) because this information should be used by manufacturing in their process DFMEA. Failure to do this was mentioned by two participants.

Failures to consider all relevant factors include not taking into account previous experience and changes to the component, and the effects these changes have on other components. Other factors include not considering the potential issues related to the materials used, to durability issues or to the effects of manufacturing tolerance.

Many participants mentioned interfaces to systems outside of the item boundary and the interactions between the item and these other systems. Comments were made that the interfaces were not correctly defined, or that interfaces were missing, or that the interfaces and resulting interaction were not properly analysed. The comments implied that these deficiencies arose because of the difficulty that the engineers had in handling interfaces and interactions, sometimes because the DFMEA was performed at too low a level of abstraction, e.g. at the component level. It was also commented that the DFMEA is less effective the more complicated the system is.

A number of participants commented that effectiveness was affected by the planning of the DFMEA. Ideally the plan should allocate sufficient time and the appropriate staff so that the DFMEA can be completed for the required programme milestone. Several comments were made to the effect that this ideal was often not met. As noted above, inadequacies in planning have a detrimental effect on team performance.

In order to judge whether an issue in the field should have been anticipated and prevented by the DFMEA, it is necessary to determine if there is a point in the DFMEA process where this failed to happen. A number of participants commented that this was not done on a systematic basis, which meant that they did not have an objective view on how effective the DFMEA process is at achieving its purpose.

The customer's perspective in terms of usage and performance was often not adequately considered, e.g. not considering all of the potential customer usage scenarios, or not verifying what the customer would accept as a satisfactory performance level.

Participants commented that they had seen DFMEAs performed at the wrong level of abstraction or DFMEAs where the analysis had not considered the design in sufficient detail

Examples of what was considered misapplication of the technique were mentioned, such as reasoning through several layers of cause-and-affect all the way through to accident sequences. If it is then decided that an accident may occur, the severity is ranked as 10. This can lead to everything being ranked as severity 10, e.g. a sun visor screw falls off into the driver's lap and they get distracted such that they lose control of the vehicle and an accident occurs.

The lack of visibility of supplier DFMEAs, or not reviewing the supplier's DFMEAs, was also mentioned as a source of missed issues.

Judgement of quality

When asked about how the quality of an DFMEA could be assessed, all agreed that it was a judgement rather than an assessment against hard criteria. Several participants mentioned assessment schemes that had been tried based on criteria such as the number of causes listed per failure mode. Some commented that these were both too detailed and too simplistic, and that a more basic assessment of the extent the process had been followed would be more useful, e.g. was quality history considered? The difficulty of assessing the quality of a DFMEA was highlighted by the example of one that was reviewed by senior staff, and considered to be a good example, however the corresponding component later experienced many field issues due to many customer usage scenarios not having been considered.

In practice, it appears that the judgement is based on inspection of the DFMEA work sheet based on ad hoc criteria, Table 25, and considering the previous experience of the product in the case of a reapplication, Table 26.

Are functions related to customer requirements?
Have obvious failure modes been missed?
Are the standards specified as controls appropriate?
Have the standards specified as controls been effective in the past
Does the worksheet capture learning about the product

Table 25: Questions asked of the DFMEA Worksheet

Warranty
Field issues
Problems before production
Test & validation results

Table 26: Previous product experience considered

It was acknowledged that the judgement is influenced by the risk assessment scores, in that higher risk scores are judged against stricter criteria. The judgement is also influenced by the quality of the overall presentation, for example, the level of detail, the consistency of the analysis, the presence of obvious mistakes, and the degree of repetition.

5.4 Discussion

The research question explored here has aimed to understand the established role and practice of using DFMEA in an automotive context and examine the factors that influence its judged effectiveness. The question arose from a desire to extend the safety case required by ISO 26262 to a *mechatronic system* by including the mechanical causes of the malfunctioning behaviour of the *Item* identified by the ISO 26262 hazard and risk assessment process. The DFMEA technique was chosen because this is at the core of the quality processes used by the automotive industry to address negative customer experiences associated with mechanical components.

So, the first result of interest is whether or not the practitioners of DFMEA view its role in a way that is amenable to being used to support an extended ISO 26262 safety argument. As recorded in Table 16, a number of common themes were apparent when the participants considered the role of the DFMEA which are all supportive of identifying and mitigating failures.

For the DFMEA to properly fulfil the new role it will have to supply evidence that, for mechanical causes of malfunctioning behaviour, a complete set of requirements have been identified, the controls are sufficient mitigation for the causes and/or effects, the product satisfies the requirements and that the process and people are appropriate.

In DFMEA terms, the requirements are the prevention and detection controls. To claim that a complete set of requirements has been identified, it is necessary to argue that the coverage of functions, interfaces, causes and effects is sufficient. Any criteria, evidence, reasoning, *etc* that supports this claim is something that could potentially be used to support an argument. Many of the answers given could provide such support. For example, many of the characteristics of a well-performed DFMEA, listed in Table 17, are topics that could directly support a completeness claim. One characteristic mentioned is that everything should be based around functions with a good functional breakdown in a logical sequence; this can be phrased as a claim such as "*The item is analysed using a logical functional decomposition"*. The evidence to support such a claim could be a diagram showing a systematic breakdown of the functions of the item. Other characteristics mentioned could give confidence in the results. For example, the involvement of stakeholders can be phrased as a claim such as "*All relevant stakeholders were involved in performing the DFMEA"*. The evidence to support such a claim could be the list of team members, their roles and the departments they represent.

To claim that the controls specified are sufficient mitigation for the causes and/or effects it is necessary to argue that the controls will be effective. To the extent that the specification of controls is dependent on the scores and classification, these also need to be justified. Some of the answers recorded in Table 25 and Table 26 are topics that could support a claim of sufficient mitigation. For example, previous experience with standards could become a claim that "*The standards specified as controls have been effective in the past"* and evidence to support such a claim could be warranty records or problem reports on products were the controls have been used previously.

To claim that the product satisfies the requirements it is necessary to argue that controls in the form of design standards, verification methods and cascaded requirements have been followed and implemented in the final product; this includes the specification, and successful completion, of tests or other verification activities. An example of the claim that we would like to make is "*All controls have been implemented in the final product and all cascaded requirements have been properly acted upon"*. While the answers given did not mention topics that could directly support such a claim, where the specified controls took the form of design standards with associated verification activities, the reports of the latter would provide relevant evidence.

5.5 Summary

In Chapter 4 we raised two issues. One issue was whether the DFMEA, as actually practiced, would be able to provide the evidence we require. From the results of the case study it can be seen that it does have the potential, but, for this potential to be realised, strong governance is required to avoid the issues highlighted in section 5.3.4. Possible extensions to this case study are discussed in 7.7.3.

We mentioned in section 5.1 that we were also interested to understand if the use of the DFMEA would benefit from having an assurance case structure. The study has revealed that there is variation in the understanding of role and of the completion criteria. There are also numerous factors mentioned that affect a successful outcome. Up to now this does not seem to have been too detrimental, perhaps because the majority of the systems were not safety related or that complex. However, systems are now becoming more complex especially with the addition of *E/E system* control. So, there may well be benefit to be gained by having a more structured way to record the results and the reasoning.

The second issue was how the concept of design integrity could be fed into the mechanical design process. This problem is now addressed in Chapter 6.

Chapter 6 Relating Mechatronic Safety Evidence

As discussed in, Chapter 2, section 2.4 Safety Arguments, a generic safety argument is based on:

- an assessment of unmitigated risk
- the derivation of safety behavioural requirements
- the implementation of safety requirements with an integrity commensurate with the unmitigated risk

In this chapter we propose a means of separating out the two meanings of the ISO 26262 term *ASIL* which are: an indication of the assessed unmitigated risk, and the integrity with which safety requirements are to be implemented. This is necessary to allow us to feed the concept of integrity into the mechanical design. We do this based on a conditional probability risk model; this allows us to show how safety requirements, with assigned integrity values, can flow down from the highest level of system description to the implementation. We also propose the use of *special characteristics* as a means of feeding integrity values into the DFMEA quality-based processes used in mechanical engineering.

6.1 Conditional Probability Risk Model

A conditional probability risk model is presented which will be used to describe the assessment of unmitigated risk and the provision of risk mitigation in the context of ISO 26262.

When a machine fails in a way that leads to harm to a person, there is a chain of cause and effect from an initial fault to the resultant harm to the person. The risk associated with this event is assessed by considering two factors: the likelihood that the harm will occur, and the severity of that harm. The likelihood that the harm will occur can be broken down into a number of cause-effect factors, for example:

- The likelihood that the fault will occur
- The likelihood that the fault will propagate so as to affect the behaviour of the machine
- The likelihood that the behaviour of the machine will interact with the environment and people, such that people are harmed

We can model the probability[3] of harm, P_{harm}, mathematically as the product of the conditional probabilities for each cause-effect factor:

$$P_{harm} = P_{fault} * P[faulty\text{-}machine\text{-}behaviour \mid fault] * P[harm \mid faulty\text{-}machine\text{-}behaviour]$$

With this understanding, we can draw a generic bow-tie diagram, Figure 76.

[3] We are using the terminology of probability to explain a concept. Numbers will not be assigned to any of these probabilities.

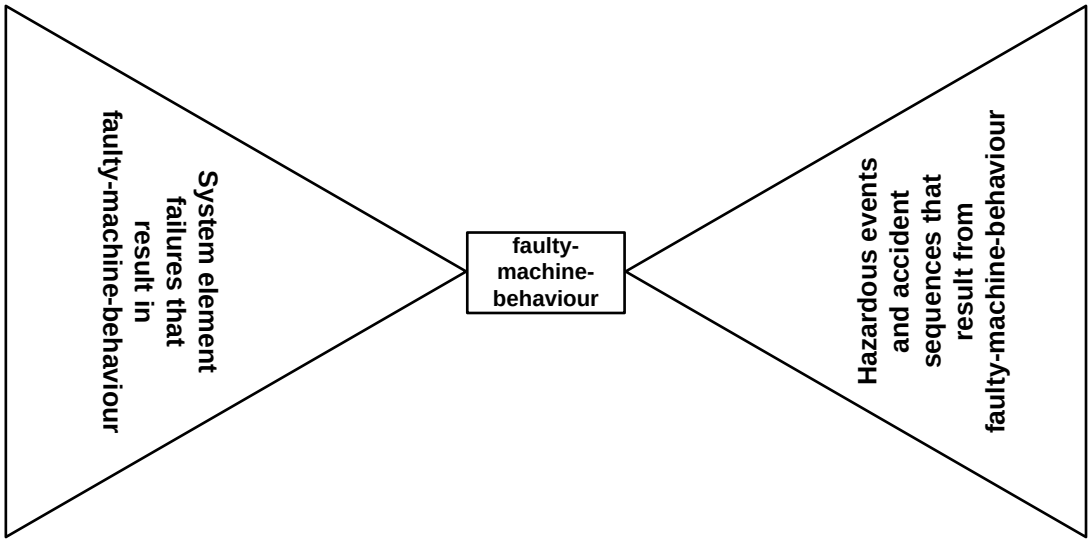

Figure 76: Fault to harm model

The faulty-machine-behaviour is in the middle. The left-hand side represents the fact that there may be many initial faults that propagate through to a particular *faulty-machine-behaviour*; this accounts for the P_{fault} * *P[faulty-machine-behaviour | fault]* terms in our mathematical model. The right-hand side represents the fact that the *faulty-machine-behaviour* may interact with the environment and people in many different ways leading to different harms; this accounts for the *P[harm | faulty-machine-behaviour]* term in our mathematical model. The severity of harm associated with the *faulty-machine-behaviour* is taken to be the worst case of all the possible outcomes of the *faulty-machine-behaviour* interaction with the environment and people.

6.2 Unmitigated Risk Assessment

We propose that the ISO 26262 scheme for assessing the unmitigated risk of an *E/E system* is also used to assess the unmitigated risk of a *mechatronic system*. For ISO 26262, the *faulty-machine-behaviour* is the *hazard*, and the hazard and risk assessment assumes that the *hazard* has occurred and assesses the consequent risk. In terms of the mathematical model, P_{fault} * *P[hazard | fault]* is assigned a value of 1, and the value of *P[harm | faulty-machine-behaviour]* is assessed. The assessment is made by considering the consequences of the *hazard* in a number of *operational situations*. Each combination of a *hazard* and an *operational situation* is referred to as a *hazardous event*. Each consequence is assigned a *severity* rating. The probability of the vehicle entering the *operational situation* is assigned an *exposure* rating and the probability that human actions can avoid the harm associated with the consequence is assigned a *controllability* rating. The result of the assessment is the tuple *{exposure, controllability, severity}* where *exposure* takes values of *E0* to *E4*, *controllability* takes values of *C0* to *C3*, and *severity* takes values of *S0* to *S3*. Using the ISO 26262 risk table, this gives the assessment of the unmitigated risk as one of the following

values: *QM, ASILA, ASILB, ASILC* and *ASILD*. These values have a universal interpretation in the context of a development conforming to ISO 26262.

Our justification for using the ISO 26262 scheme risk to assess a *mechatronic system* is that in practice the assessment of the *E/E system* has always had to take into account the capabilities of the actuators, or their assumed capabilities, and their effects on the mechanical components. The magnitude of these effects (e.g. torque output, force exerted, speed of operation, brightness, loudness), or their estimates, are necessary to determine values of *severity* and *controllability*.

In the mechatronic example given in Chapter 4, the assessment of unmitigated risk is the subject matter of *Pars 1,* and design artefacts produced are the same as for an *E/E system* except for a name change.

6.3 Integrity levels

The P_{fault} term in the conditional probability risk model is handled by ISO 26262 with the concept of an integrity level, Chapter 22.3.3 Product Safety – Levels, which is assigned to safety requirements. The P_{fault} term includes the probability of occurrence of both systematic and random causes of faults. By assigning an integrity level to the safety requirements, ISO 26262 is indirectly specifying process measures, referred to here as *process tailoring*, whose aim is to reduce P_{fault} to an acceptable value, although this is never expressed as a number. *Process tailoring* is discussed further in section 6.5. ISO 26262 uses the same term, *ASIL*, to indicate both the unmitigated risk associated with the *item* and the integrity with which a safety requirement is to be implemented.

However, as noted in Chapter 4, there is a problem in applying the ISO 26262 framework to a *mechatronic system* because a value of *ASIL* cannot be assigned to safety requirements placed on the mechanical elements of the architecture. We now start to describe a proposed solution to this problem. The first step is to replace the use of *ASIL* to indicate the value of the unmitigated risk with a more generic term, R_{Um}, so the ISO 26262 risk table (part-3, Table 4), is now as shown in Table 27. This approach is similar to that used in the MISRA Safety Analysis Guidelines, [52]. It is also used in edition 2 of ISO 26262, where the unmitigated risk of a motorcycle *hazard* is assigned an *MSIL* value and this is then mapped to a value of *ASIL* to indicate the integrity required of the mitigation measures required. The use of the R_{Um} terms will be explained in the following sections. Note, the values of *S0*, *E0* and *C0* do not appear in the table because ISO 26262 does not complete a risk assessment if one of these values is assigned.

6.4 Risk Mitigation Strategy

The first stage in risk mitigation is to define a strategy for handling the right-hand side of the bow-tie diagram. Risk mitigation may be achieved by addressing the *P[harm | faulty-machine-behaviour]* term of the risk model or by addressing the severity of the consequence. Adapting the

terminology of ISO 26262, this involves the definition of a *mechatronic safety goal* followed by the specification of a *mechatronic functional safety concept*. Following the ISO 26262 approach, the concept of *process tailoring* is not applied when defining the risk mitigation strategy and the same process is followed irrespective of the R_{Um} values assigned to the *mechatronic safety goals*.

Severity Class	Exposure Class	Controllability Class		
		C1	C2	C3
S1	E1	$R_{Um}1$	$R_{Um}1$	$R_{Um}1$
	E2	$R_{Um}1$	$R_{Um}1$	$R_{Um}1$
	E3	$R_{Um}1$	$R_{Um}1$	$R_{Um}2$
	E4	$R_{Um}1$	$R_{Um}2$	$R_{Um}3$
S2	E1	$R_{Um}1$	$R_{Um}1$	$R_{Um}1$
	E2	$R_{Um}1$	$R_{Um}1$	$R_{Um}2$
	E3	$R_{Um}1$	$R_{Um}2$	$R_{Um}3$
	E4	$R_{Um}2$	$R_{Um}3$	$R_{Um}4$
S3	E1	$R_{Um}1$	$R_{Um}1$	$R_{Um}2$
	E2	$R_{Um}1$	$R_{Um}2$	$R_{Um}3$
	E3	$R_{Um}2$	$R_{Um}3$	$R_{Um}4$
	E4	$R_{Um}3$	$R_{Um}4$	$R_{Um}5$

Table 27: Redrafted ISO 26262 Risk Table

6.4.1 Mechatronic Safety Goals

A mechatronic safety goal is a top-level safety requirement associated with one or more *hazardous events*. If it is met, then the potential for unreasonable risk of its associated *hazardous events* is avoided. It is expressed as a functional objective and is the basis on which functional safety requirements are determined. In practice, there are two styles of defining these goals; one is in terms of system behaviour, for example, entering a safe state or constraining nominal behaviour and the other is defining the goal as a statement that unreasonable risk shall be avoided. The significance of this is discussed below. The *mechatronic safety goals* are assigned a value of R_{Um} which is taken as the worst case value from their associated *hazardous events*. In the Chapter 4 example, the *mechatronic safety goals* are defined in *Pars 1*. The process and design artefacts required by ISO 26262 are applicable to the *mechatronic system*.

6.4.2 Mechatronic Functional Safety Concept

A *mechatronic functional safety concept* is intended to achieve the *mechatronic safety goals* with which it is associated. It may be based on entering a safe state or constraining nominal behaviour, for example:

- Warnings to the driver to prompt actions to maintain control which reduce the value of *controllability*
- Changes to vehicle behaviour to allow the driver to maintain control which reduce the value of *controllability*

- Changes to vehicle behaviour to prevent entry into, or to exit from, the *hazardous event* which reduce the value of *exposure*
- Reduction of the magnitude of the effect to reduce the value of *severity*

The concept is defined by allocating *mechatronic functional safety requirements* to elements of the *mechatronic system architecture*. The significant change for the *mechatronic system* is that the concept now explicitly includes the mechanical design as described as a function structure in the *Mechanical Architecture*, see Chapter 2, section 2.1.4 Mechanical Design. The established mechanical engineering design approaches to safety, as described in Chapter 2, section 2.3.3Product Safety - Mechanical Design, are now considered to be part of the *mechatronic functional safety concept*. This is not the case for an *E/E system* development where any relevant mechanical aspects would only have been documented in the *item definition*. The *mechatronic functional safety requirements* are assigned a value of R_{Um} which is taken as the worst case value from their associated *mechatronic safety goals*. The *mechatronic functional safety concept* can still allocate safety requirements to *external measures* which can be an *E/E system* or non-E/E technology. The latter do not have a R_{Um} value associated with them, so the sense of integrity required of the design and implementation of the measures is not considered as it is out of scope.

In the Chapter 4 example, the *mechatronic functional safety concept* is defined in *Pars 2*. The process and design artefacts required by ISO 26262 are applicable to the *mechatronic system*; some of the artefacts have been renamed but the content has not substantively changed.

The aim of the risk mitigation strategy is to avoid any unreasonable risk which was identified by the assessment of the unmitigated risk. Therefore, the sufficiency of the risk mitigation strategy has to be argued based on its ability to avoid unreasonable risk. The argument may be based on the definition of the *mechatronic safety goals* if these are defined in terms of system behaviour. If the goals are a statement that unreasonable risk shall be avoided, then the argument has to be based on the *mechatronic functional safety concept*. In the MISRA framework, [200], the argument is made for the *safety goals* which define the required top level system behaviour. The sufficiency of the risk mitigation is demonstrated by using the ISO 26262 risk assessment scheme to assess the residual risk associated with the *item*, assuming that the top level system behaviour has been achieved. This approach is adopted here for the *mechatronic system*.

6.5 Risk Mitigation Implementation

The design proceeds by the derivation and implementation of the safety requirements at the different design levels and across the different technologies so that together they result in the defined strategy being achieved. In the mechatronic example of *Chapter 4*, these are *Pars 3 Mechatronic Technical Safety Concept, Pars 4: E/E System Technical Safety Concept, Pars 5 Hardware Design, Pars 6*

Software Design and *Pars 7 Mechanical Design*. The safety requirements in each *Pars* are derived from the information cascaded to them from other *Partes* and from analysis of the design performed in the *Pars*.

Systematic faults may occur in the derivation and implementation of the safety requirements. Random faults may occur due to hardware failures. In terms of the conditional probability risk model, we are considering the left-hand side of the bow-tie diagram, $P_{fault} * P[hazard \mid fault]$. The P_{fault} term covers the occurrence of both the systematic and random faults; this is addressed by the concept of integrity levels as described above. The *P[hazard | fault]* covers the possibility of a fault resulting in a *hazard*; this is addressed by an analysis of the design at each level to understand how faults result in failures which cascade from one element of the design to another. Based on this understanding, safety requirements are specified for the detection of faults, or failures, and for a system response in compliance with the *mechatronic functional safety concept*.

To apply the ISO 26262 *process tailoring* to the *E/E system*-related *Partes* (4, 5 and 6) we need to map the values of R_{Um} to *ASILs*, representing the integrity with which the safety requirements are implemented. This allows the P_{fault} term to be addressed for these *Partes*. This a trivial task as the R_{Um} values were defined as direct replacements for the *ASIL* values in the ISO 26262 table, where they are first defined as an indication of the unmitigated risk.

For *Pars 7 mechanical design*, we have the problem highlighted in Chapter 4. The challenge is to have a practical means of including the concept of integrity in the DFMEA quality-based processes used in mechanical engineering. There are two issues, a means of communicating a value of integrity and an interpretation of the value it a manner that can be acted upon in the context of the DFMEA. The latter is a challenge because of the range of technologies, their failure modes and their associated design practices. Any proposed scheme has to be sufficient general to allow it to be applicable to a wide range of technologies. Our approach is to use a very general scheme.

Our proposed means of addressing the first issue to use s*pecial characteristics*. A DFMEA is usually a means of identifying a s*pecial characteristic*, here we propose a different use whereby the s*pecial characteristic* is identified by the assessment of the unmitigated risk. As an example, we propose a mapping from R_{Um} values to an arbitrary set of s*pecial characteristics* ($SS_{SC}1$, $SS_{SC}2$, $SS_{SC}3$, $SS_{SC}4$, $SS_{SC}5$) as shown in Table 28, along with the mapping of R_{Um} values to ASIL values. Five s*pecial characteristics* have been designated to match the five values of unmitigated risk. The proposed use of these designations is explained in section 6.5.3.

6.5.1 Mechatronic Technical Safety Concept

The specification of a *mechatronic technical safety concept* is a new stage that we introduced in the Chapter 4 example to allow the *mechatronic functional requirements* to be allocated to elements of

the mechanical and E/E designs. The significance of the change is that safety requirements are explicitly cascaded to the mechanical design, whereas for an *E/E system* the *item definition* only records any relevant assumptions about the mechanical design. The *mechatronic technical safety requirements* are assigned a value of R_{Um} which is taken as the worst case value from their associated *mechatronic technical safety requirements*.

Inherent Conceptual Operational Risk	E/E System Requirement Integrity Attribute	Mechanical Component Design DFMEA Special Characteristics
$R_{Um}1$	QM	$SS_{SC}1$
$R_{Um}2$	ASILA	$SS_{SC}2$
$R_{Um}3$	ASILB	$SS_{SC}3$
$R_{Um}4$	ASILC	$SS_{SC}4$
$R_{Um}5$	ASILD	$SS_{SC}5$

Table 28: Mapping Risk to Integrity requirements

Although there is not direct equivalent in ISO 26262, it was possible to reapply the artefacts and properties from *E/E system* design. While ISO 26262 does support *process tailoring* for the *E/E system* design, we do not attempt to define any tailoring here as the result would be purely arbitrary. However, some of the system testing that is performed in the *E/E system Pars* will now be performed in the *mechatronic technical safety concept Pars*; this testing is tailored so this could form the basis on which tailoring is brought into this *Pars*. We do not advocate tailoring for derivation of the *mechatronic technical safety requirements* as these are seen as being just as significant for the overall safety case as the *mechatronic functional safety requirements* for which there is no process tailoring.

6.5.2 E/E System Design

In Chapter 4 we saw that *Pars 4*, *Pars 5* and *Pars 6* are similar to the equivalents for an *E/E system.* Therefore, the process, artefacts and properties defined by ISO 26262 can all be reused in this context. The *process tailoring* to achieve the required integrity, as indicated by the *ASIL* value assigned to the safety requirements, is defined in the relevant parts of ISO 26262. The process requirements of ISO 26262 achieve the required integrity by being tailored depending on the *ASIL* value of the safety requirements that they are handling. The tailoring works by having some of the clauses of the standard only applicable to higher values of *ASILs*, or by having the strength of the recommendation to use particular techniques, to establish the properties of artefact, dependent of the value of *ASIL*.

6.5.3 Mechanical Design

In Chapter 4 for *Pars 7 Mechanical Design*, we identified robustness as a key property pertinent to the safety argument. The robustness property will be established by the use of the DFMEA, or broader failure mode avoidance process based on the DFMEA, see Chapter 2, section 2.3.2 Product

Quality. In this section we will describe how the concept of integrity can be brought into the DMFEA process through the use of *special characteristics*.

First, we contrast our proposal for the mechanical design with that of the *E/E system* design. For an *E/E system*, safety requirements, with assigned integrity values, are allocated to an element of the architecture. These are then implemented and verified in a design using a process consistent with the integrity values of the safety requirements. For a mechanical design, safety requirements, with assigned integrity values, are allocated to a mechanical element of the architecture. These are then implemented in a design and the design analysed using a DFMEA. For those failure modes that would cause a safety requirement not to be met, design controls are applied in accordance with the integrity value of the safety requirement that would be violated.

Pars 7 has *mechatronic technical safety requirements* cascaded to it. We propose that these safety requirements have values of R_{Um} assigned to them. A mechanical design is created to fulfil both the nominal behaviour requirements and the *mechatronic technical safety requirements*. The design is analysed using a DFMEA.

Below we describe how the use of the DFMEA fits in with the condition probability risk model and how *special characteristics* could be used as a means to bring the concept of integrity into the DFMEA process. A fuller description of *special characteristics* in general is given along with suggestions for defining a meaningful interpretation of them for achieving integrity.

DFMEA and the conditional probability risk model

As described in Appendix A, the DFMEA models the subject of analysis as a set of functions; for each function it assesses the *effects* of each of its *failure modes* and determines possible *causes* of the *failure mode*. In the bow-tie diagram, Figure 76, the *effect* is the *faulty-machine-behaviour*. The likelihood of the *effect* occurring is assessed by assigning an *occurrence ranking* to the cause of the *failure mode* and a *detection ranking* to the cause of the *failure mode* and/or the *failure mode* itself. These rankings are effectively estimating $P_{fault} * P[Effect \mid fault]$, but this estimation is not an absolute value, but rather is a value that is relative to the subject of analysis. This accounts for the $P_{fault} * P[faulty\text{-}machine\text{-}behaviour \mid fault]$ term in our mathematical model, 6.1.

The $P[harm \mid effect]$ term is not formally evaluated in the DFMEA. A binary decision is made as to whether or not the effect has the capacity to cause harm based on a consideration of the *severity ranking*, with a value of 10 being assigned if the team consider that the *effect* meets the criteria given, e.g. potential failure mode affects safe vehicle operation, [159]. Unlike the ISO 26262 scheme, this is no systematic analysis of the failure mode in different operating situations, this means that consequences with lower values of unmitigated risk may not be identified. The value may be reduced to 9 if the driver is warned of the effect or failure and it is deemed that they have

time to act to prevent the harm occurring. So in the evaluation of P_{harm}, P_{fault} * *P[effect | fault]* is represented by a tuple *{occurrence ranking, detection ranking}* and *P[harm | effect]* is assigned a value of 0 or 1. The *occurrence ranking* and *detection ranking* take values of 1 to 10, but these have no universal interpretation as the rankings are relative to the subject of the analysis.

The DFMEA seeks to reduce the P_{fault} and *P[effect | fault]* terms by the use of *Prevention Design Controls* and *Detection Design Controls*. *Prevention Design Controls* can include means to detect and manage *causes* or *failure modes* during normal operation; adapting the ISO 26262 terminology, these are part of the *mechatronic functional safety concept*. The *severity ranking* can be changed if the *cause* or the *failure mode* can be eliminated by the *Prevention Design Controls* and *Detection Design Controls*.

As has been noted, in most instances the DFMEA is revealing issues related to customer convenience rather that customer safety. There will be times when the safety and customer convenience arguments will be in conflict with each other, for example the use of an interlock to prevent vehicle movement if a seat belt is not being used. The debates around such issues are legitimate and the fact that, under our proposal, the safety aspects will be made more visible will only lead to a more informed debate.

Relating the DFMEA Results to the Assessment of Unmitigated Risk

We propose two linking mechanisms for relating the results of the DFMEA to the assessment of the unmitigated risk.

The DFMEA identifies *failure modes*, their *effects* and their *causes*. The *effects* will be identified at the boundary of the design and also on the final product, in this case the vehicle. The *effects* will be assigned a *severity ranking*, a vehicle level *effect* that is deemed to be safety related which will be assigned value of 9 or 10. A value of 10 may be designated as a critical characteristic which is an example of the normal use of a *special characteristic*. In our proposal, such vehicle level *effects* would be cascaded to *Pars 1* for comparison with the set of identified hazards. If the *effect* represents a new *hazard*, then the risk assessment is updated and, if necessary, revised *mechatronic safety goals* are cascaded to *Pars 2.* This is the first proposed mechanism for relating the results of the DFMEA to the assessment of the unmitigated risk.

We also propose that the *effects* identified by the DFMEA at the boundary of the design be related to the *mechatronic technical safety requirements* implemented by the design. If an *effect* causes one of the safety requirements to be violated then the *severity ranking* of the *effect* would be set to a value of 10 regardless of the ranking assigned in the DFMEA. In these cases it is more appropriate for the severity to be defined top-down rather than inductively from the component; this would ensure a level of consistency that is not traditionally sort. The value of the unmitigated risk assigned

to the safety requirements would be translated into a SS_{SC} value. This value would mandate the use of defined *prevention controls* and *detection controls* as described in the next section.

Special Characteristics

The quality standard, IATF 16949:2016, [143] is universally used in the automotive industry and certification by external auditors is usually obtained. It requires the use of FMEA and it also calls for *special characteristics* to be identified and acted on. *Special characteristics* are defined as "*those characteristics of the design that are crucial to the safe and proper functioning of the product"* and the use of FMEA is acknowledged as a technique by which they can be identified. SAE J1739, [159], and the VDA standard, [172], also acknowledge that the technique can be used to identify *special characteristics*. ISO 26262 also recognises safety-related *special characteristics* which defines as a "*characteristic of an item or an element, or else their production process, for which reasonably foreseeable deviation could impact, contribute to, or cause any potential reduction of functional safety"*.

Given the definition of a *special characteristic*, it seems eminently suitable as a means of linking the concept of integrity from the functional safety process into the quality management process. *Special characteristics* are normally created by a DFMEA, see Appendix A, but in this proposed usage, they are created by design and feed into the DFMEA.

Interpreting Special Characterises as Integrity

In Table 28, five different *special characteristics* are listed, but in practice each organisation would decide how many they needed and how they mapped to values of R_{Um}. Although five have been listed to match the number of levels of unmitigated risk, in practice it is unlikely that it would be practical to define five different levels of integrity in every circumstance.

In our proposal, each *special characteristic* would be defined to state criteria against which the sufficiency of the *Prevention Design Controls* and *Detection Design Controls* could be judged. The use of the design controls in this way is our proposed way of introducing the concept of integrity into the mechanical domain. In this way we are avoiding the functional safety approach of the having a whole process defined in terms of different integrity values and we are building on what is already established practice.

Defining the criteria for each *special characteristic* would not be a simple task. One approach could be based on comparing the mechanical practice for those systems that have always been seen as safety related, e.g. brakes and steering, and relating this to the ASIL value of the associated E/E controller. This could then be taken as a benchmark for other mechanical systems whose E/E controllers have the same ASIL value.

It may be possible to abstract out certain aspects of the development that are common to both the mechanical design and the *E/E system* design, e.g. testing. The requirements of the ASIL value should be consistent with those of the associated *special characteristic*, in the case of the testing, we would expect both domains to be performing comparable levels of testing.

The FMEA standards provide examples of design controls. SAE J1739, [159], gives the example design controls shown in Table 29. One can see that the standards used, or the rigour with which the techniques are applied could be varied to provide different levels of integrity.

Prevention Controls	**Detection Controls**
Use of published design standards	Use of finite Element Analysis
Use of heat treatment specification	Use of CAE analytics
Use of redundant design measures, e.g. sensor shield	Use of tolerance stack analysis
Use of corporate best practice standard designs	Use of validation testing (fatigue, water intrusion, vibration, ride and handling, etc.)
Use of system detection and driver notification for servicing	
Use of system detection and operational status display to driver	

Table 29: SAE J1739 Example Design Controls

The VDA standard, [172], gives the use of simulation and tolerance calculation as examples of *Preventative Actions*. For *Detection Actions* it gives examples of the use of simulation, test plan rigour and the rigor of the drawing checks. Again, one can see that varying the rigour with which the techniques are applied could be used to provide different levels of integrity.

The results of the DFMEA case study may also provide criteria that could be used in the definition of the *special characteristics*. Table 17 listed the characteristics of a well performed DFMEA, from these, potential subjects that could be used as the basis for defining different levels of integrity are shown in Table 30

Requirements for stakeholder involvement
The rigour with which the functions are defined through logical decomposition
The rigour with which functions are related to customer requirements
The degree to which the function definitions are defined in scientific or engineering terms specific to the component
The use of the different failure mode types
The number of cause that have to be considered for each failure mode
The mandatory use of design standards as controls
The rigour with which Prevention Controls are linked to the design requirements specification
The use of test standards as controls
The rigour with which the product development is documented

Table 30: Potential Integrity Subjects based on a well performed DFMEA

Table 18 lists completion criteria; from these, the rigour of the review could be used as the basis for defining different levels of integrity are shown in Table 31. Some of these may be a binary decision to perform the check or not.

Check that all the correct controls are in place and actioned
Check that the risk assessment scores
Check the analysis has been performed to the appropriate depth
Perform a system review

Table 31: Potential Integrity Subjects based on a Complete Review

It may also be possible use the *special characteristic* definitions to prescribe the rigour with which the quality processes mentioned in Chapter 2, section 2.3.2 Product Quality, are applied. It may also be possible use the *special characteristic* definitions to specify the use of safety factors in the mechanical design, see Chapter 2, section 2.3.3 Product Safety.

The use of subjects like those mentioned above to define integrity would need to be carefully calibrated to achieve the required integrity while remaining practical. This calibration would have to be established over a period of time by feeding back actual experience into the process. We should stress that this proposal is an example scheme.

A diagram showing the flow of requirements and their integrity values is shown in Figure 77.

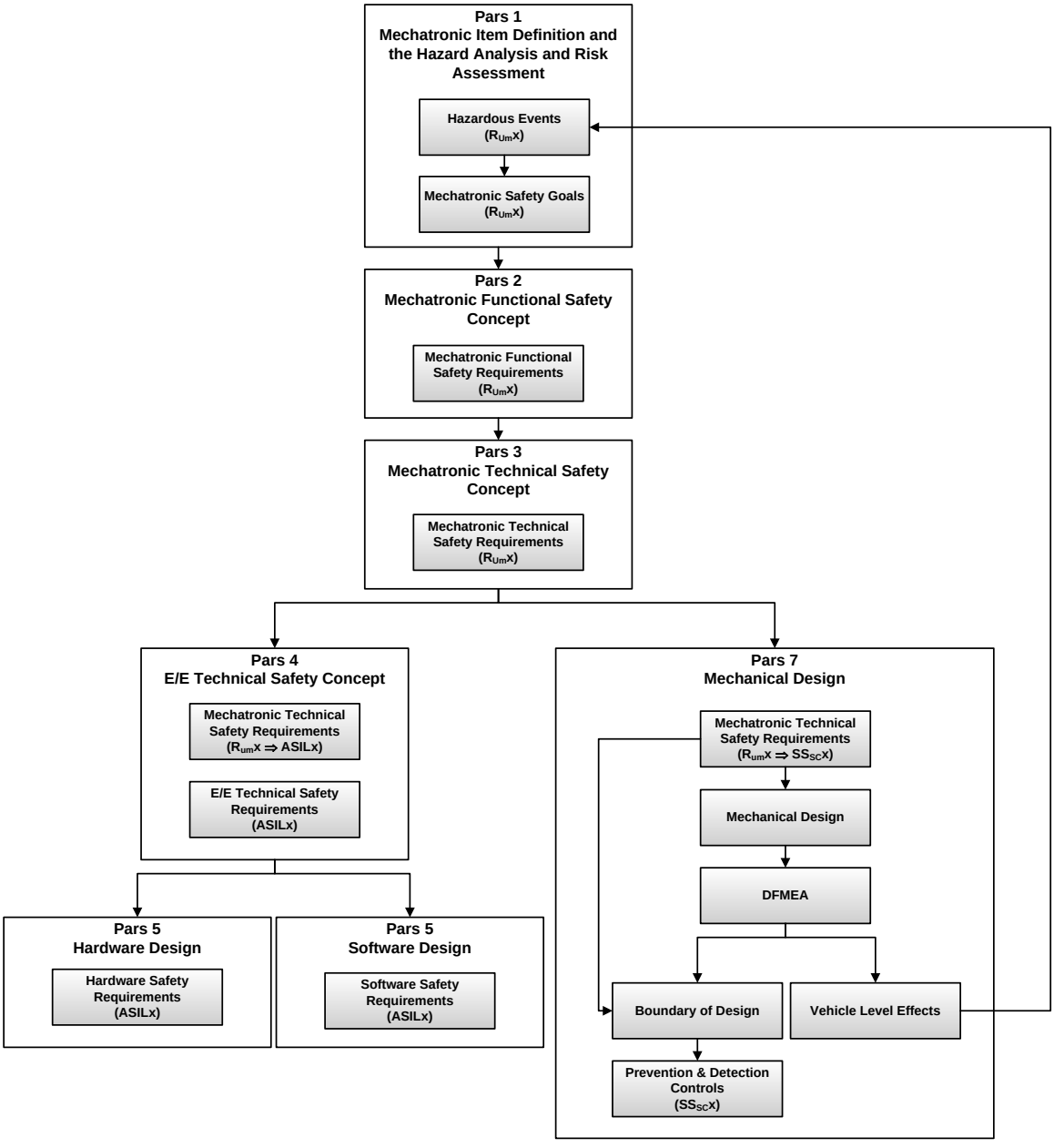

Figure 77: Cascade of requirements and integrity values

6.6 Alternative sufficiency criteria

Given that reliability engineering is well-established in the mechanical design, [177], [176], the question arises as to why this is not used as a sufficiency criteria. There are two issues regarding its use. One is that the functional safety approach is not based on meeting a probabilistic occurrence value for a safety goal; even the ISO 26262 target values for hardware metrics are chosen by the designer. The other is the general understanding that for complex software-based systems, errors in the derivation and implementation of safety requirements are just as significant, if not more, than the random failures covered by reliability engineering. As we saw in Chapter 2, the use of *Probabilistic Risk Assessment* (PRA) has been strongly criticised by Leveson, [75].

6.7 Summary of overall scheme

In this chapter we have proposed a scheme for flowing down safety requirements, with assigned integrity values, from the highest level of system description to the implementation, Figure 77. We have shown how the risk assessment of the functional safety process relates to that of the DFMEA through the conditional *probability risk model*. We have separated out the two meanings of the ISO 26262 *ASIL*, which has allowed us to feed integrity values, derived from the risk assessment, into the DFMEA quality-based processes used in mechanical engineering.

There are steps in the process that have not been fully worked out. We have not proposed any *process tailoring* for the *Mechatronic Technical Safety Concept*, *Pars 3*, although to be consistent with ISO 26262 the testing performed here would have some tailoring based on the require integrity. We have only suggested possible sources for the definition of the SS_{SC} values and it will be a non-trivial task to define these.

In practice, it is unlikely that the R_{Um} terminology would be adopted because the language of *ASIL* is now so deeply entrenched within the automotive industry. This does not invalidate the scheme as ASIL values can still be mapped to SS_{SC} values

Chapter 7 Evaluation

7.1 Introduction

The research objective stated in Chapter 1 is to establish a uniform approach to justifying that an automotive *mechatronic system* is fit to be put into production from a "functional safety" perspective. The intention is to extend the existing work on automotive safety arguments for *E/E systems* which is based around a product requirements decomposition over a generic view of the system design through levels of design abstraction. Consequently, it was necessary to have a *mechatronic system* equivalent of the generic *E/E system* levels of design abstraction which can be used as the basis for requirements decomposition, and on which a safety argument can be constructed that includes the design of the mechanical elements of the system. A number of specific thesis objectives were defined to achieve this:

- TO1: To establish a design representation upon which a safety argument can be based
- TO2: To establish a safety argument pattern based on the design representation
- TO3: To establish a linkage of functional safety integrity to mechanical development
- TO4: To establish a means of providing evidence to support claims related to mechanical development

In this chapter we describe and evaluate work done on each of these thesis objectives in turn. We describe the further evaluation that can be performed and finally state what contributions have been achieved in this work.

7.2 TO1: To establish a design representation

Research Approach

The motivation was to have a pattern for representing levels of *mechatronic system* design abstraction that was not just an extension of existing patterns for an *E/E system*, e.g. the MISRA framework, [200]. We were conscious that in practice the work would be divided between many different parties, e.g. departments, companies, and that a pattern would have to be based on something that recognised this division. This led naturally to this first thesis objective to find a suitable pattern for representing the division of work for the development of a *mechatronic system*.

The initial approach to finding a suitable pattern was to review the literature on general systems engineering, *mechatronic systems*, *mechanical design* and *E/E system design*. However, we were unable to find a suitable means of describing a system as a decomposition through levels of design abstraction upon which a safety argument could be constructed. The literature review also confirmed that there is no equivalent in the mechanical design process of the concept of integrity levels, which is fundamental to the functional safety standards.

Consequently, it was necessary to produce our own description, which we term the *Pars* approach. The development of this is explained in section 3.1 onwards. The *Pars* approach is based on defining a generic model for engineering development that can be applied at any level of abstraction. The model consists of an ontology, a process and an argument pattern. The ontology defines logical entities, physical entities and their relationships. To use the *Pars* approach, system development is divided into a set of appropriate abstraction levels and an ontology for a *Pars* is defined at each abstraction level based on the generic model. The process covers the production of the entities defined by the ontology.

Note, although we are using the phrase "abstraction levels" as the means to divide system development, as noted in section 3.2.2, in practice the division may be at the same level of abstraction but cover different technologies, e.g. *E/E system* development and mechanical development.

In our usage of the *Pars* approach, a set of *Partes* is first defined for a generic system, e.g. *E/E system*, *mechatronic system*, and then the generic system set of *Partes* is instantiated for a particular system. In our example we have instantiated the generic *mechatronic system* set of *Partes* for a Four Corner Air Suspension system.

Evaluation

The *Pars* approach is a theoretical conjecture whose validity can be contested. For example, are the entities defined in the ontology sufficient to describe a real system that has been divided into a set of abstraction levels? Also, are the relationships the right ones and do they hold in practice? To provide some confidence that the *Pars* approach works in practice a number of evaluations were performed:

- Evaluation of the practicality of the *Pars* approach (Case Study 2)
- Evaluation of *Pars* ability to model an *E/E System*
- Evaluation of the ability of a *mechatronic system* represented as a set of *Partes* to map to design artefacts from an existing project, 4CAS

To evaluate the practicality of the *Pars* approach, a short case study was performed based on an example of Four Corner Air Suspension. Potential issues with the use of this example are discussed in 7.4 below. The purpose of the case study was to ascertain:

- What potential does the *Pars* approach have for accurately capturing all the information?
- What potential does the *Pars* approach have to increase overall understanding of the system?
- How practical is the *Pars* approach?

A qualitative technique of semi-structured interviews was used as the data collection instrument, [195]. General questions were asked to get an understanding of what the practitioners thought of the approach. The case study is written up in Appendix D. The overall result was positive. Staff responsible for the *E/E system* design and the mechanical system design could relate to the system described as a set of *Partes*; such an explicit representation of the development as a *mechatronic system* was seen as an improvement over current practice. Although the outcome was positive, there are limitations to the results of the case study. The sample size is small as it is necessarily restricted to staff still in the company who had worked on the project. A number of points are worth noting:

- The set of *Partes* used was a simplified version of that described in Chapter 4, so is not fully representative
- There were some practical concerns about the availability of the documents and the fact that the interplay between the different development streams is not explicitly shown on the diagram
- The cascading of a specification from one *Pars* to another was seen as being a little artificial, as it may be the same staff who produce both the initial version of the specification and also the final one
- The fact that requirements often change as a result of feedback between the *Partes* is not represented well

To determine if the entities and relationships defined in the *Pars* ontology are sufficient to capture the generic descriptions of systems given in the literature, we first applied the approach to an *E/E system* by defining a set of *Partes* based on the abstraction levels given in ISO 26262, [13], i.e. *Item definition & HARA* (including safety goals), *Functional Safety Concept*, *Technical Safety Concept*, hardware development and software development. This is described in section 3.4, and demonstrated that all the major concepts of ISO 26262, see Appendix B, could be adequately represented. That this is the case is not surprising as this model is deeply ingrained in the author's mind due to many years involvement in writing, and then applying, the standard.

A second exercise, described in section 4.2, was then performed to further assess the adequacy of the entities and relationships defined in the *Pars* ontology. In this exercise, the *Pars* approach was applied to a *mechatronic system* by defining a set of *Partes* based on the abstraction levels given in ISO 26262, [13], with the addition of one for mechanical development. Some of the ISO 26262 abstraction levels were reinterpreted for a *mechatronic system*, i.e. *Mechatronic Item Definition & HARA* (including mechatronic safety goals), *Mechatronic Functional Safety Concept*, *Mechatronic Technical Safety Concept*, *E/E Technical Safety Concept*. It was not necessary to change the definition of the *Pars* for hardware development and software development from those used to represent an *E/E system*. The definition of the *Pars* ontology for the mechanical development was based on a description given in Pahl and Beitz, [48]. The exercise demonstrated that *Partes*,

reinterpreted from their ISO 26262 equivalents, could adequately represent our division of a *mechatronic system*. The definition of the mechanical development *Pars* is more speculative and has not been subject to a review by a mechanical development specialist.

To further test the *Pars* approach, some of the *Partes* in the set for the *mechatronic system* were instantiated using the 4CAS example, i.e. the entities of the ontologies were mapped to existing design artefacts of the 4CAS project. This is described in section 4.2. Potential issues with the use of the 4CAS example are discussed in 7.6 below. The ontology was instantiated for the following *Partes, Mechatronic Item Definition & HARA* (including mechatronic safety goals), *Mechatronic Functional Safety Concept, Mechatronic Technical Safety Concept, E/E Technical Safety Concept* and the mechanical development. The evaluation using the 4CAS example in only a partial exercise; the coverage achieved against the *Pars* model is shown in Table 1Table 32 where the shaded cells indicate what was covered.

Generic Pars		Pars 1	Pars 2	Pars 3	Pars 4	Pars 5	Pars 6	Pars 7
B1	Pars Design Description	■	■	■	■			■
B2	Pars Design	■	■	■	■			■
B3	Pars Design Choice	■						
B4	Property							
B5	Verification							
B6	Aspect Cascaded to other Partes							
B7	Aspect Realized in current Pars							
B9	Physical Part Realization			■	■			■
B10	Related Physical Part							

Table 32: Coverage of Mechatronic Parts by 4CAS example

Coverage was limited because most of the ontology entities do not have associated 4CAS documentation. In some instances the necessary document did not exist, in others, e.g. requirements, the documentation is large and stored in databases that are not easy to portray in a text document. Also, the development was not planned to follow the *Pars* approach and so not all the documentation included in *Partes* ontologies would be produced by the process that was followed at the time. So, the exercise only gives a flavour of how an instantiation may look. However, it did show that, for the *Partes* involved, the existing project document could be mapped to entities of the ontology. Although not conclusive, the approach shows promise, and nothing has been revealed that shows it could not be made to work. The generic *Pars* process, given in section 3.3.2, has not been subject to any evaluation.

Conclusion

While the evaluations of the *Pars* ontology approach to representing a *mechatronic system* performed to date are only partial and not conclusive, the overall approach has not yet encountered any major obstacles to its application from a user's practicality perspective or from the partial

instantiations. We note that the *Pars* approach does not improve the situation regarding the composition of modular arguments as described in 3.3.1. Further evaluation is discussed in 7.7.1.

The *Pars* approach has some similarities with the use of a work package in project management. In project management, a work package is an independently deliverable unit linked to an organization with clear relationships to other work packages, [201]. This adds weight to the practicality of the *Pars* approach.

As mentioned in Appendix B, ISO 26262 requires that a *Functional Safety Assessment* be performed to demonstrate that functional safety has been achieved by the *item*. The standard *implies* that the assessment is performed by the owner of the *item* on the whole development. It does not address the fact that the development is always divided between different organisations, except for recognising the need for a *distributed interface agreement* and a *hardware-software interface specification*. In practice, each organisation defines its own scope for this activity and then performs a *Functional Safety Assessment* based on their scope. The owner of the *item* has the task of piecing together the different results to produce the overall assessment. The *Pars* concept was developed to explicitly acknowledge the division between organisations and should help facilitate the production of the overall assessment by having made the links between different aspects of the development explicit.

The *Pars* approach result is very generic and potentially can be applied more widely than its use in this thesis, but evaluation exercises have only been performed within the limited scope of *E/E systems* and *mechatronic systems*.

7.3 TO2: To establish a safety argument pattern

Research Approach

An argument pattern was developed as part of the development of the *Pars* approach, i.e. the argument is based around the *Pars* design ontology. This is explained in sections 3.3.3 and 3.3.4. The argument pattern is for the design, but our use of the pattern is for safety. The *Pars* approach requires a system development to be divided into a set of appropriate abstraction levels and a *Pars* ontology defined for each one. The *Pars* argument pattern is applied at each abstraction level, based on the corresponding design *Pars* ontology for that level. This allows us to adopt the MISRA cascade of safety requirements approach for the mechatronic safety argument framework while basing it on a more generic system decomposition than the ISO 26262 safety requirements cascade used by MISRA. Several papers on the MISRA framework have been presented, [200], [187], and a draft copy of the guidelines was issued for public review, [189]. The approach of basing the argument around the cascade of safety requirements across levels of abstraction has not been

challenged. This approach is accommodated by the *Pars* argument pattern because it is based on the more generic concept of properties that includes compliance with safety requirements.

In the same way that we did for the ontologies, we have defined a set of argument patterns corresponding to the *Partes* for a generic system, e.g. *E/E system*, *mechatronic system*. These then have to be instantiated for a particular system, e.g. *Four Corner Air Suspension*.

Evaluation

The *Pars* safety argument pattern is only valid if the *Pars* design ontology is valid. We have evaluated the safety argument pattern assuming that the *Pars* design ontology is valid, but this validity has only been partially established. Even assuming that the *Pars* ontology is valid, the *Pars* argument pattern is a theoretical conjecture whose validity can be contested. To provide some confidence in the validity of the *Pars* argument, two evaluation exercises were performed based on a *mechatronic system*:

- Evaluation of the *Pars* argument pattern's ability to represent a safety argument for a generic *mechatronic system*
- Evaluation of the *Pars* argument pattern's ability to represent a safety argument for a particular instantiation of a *mechatronic system* based on an existing project, 4CAS

As described in 4.2, a set of *Partes* for a generic *mechatronic system* were defined based on the abstraction levels given in ISO 26262, [13], with the addition of one for mechanical development. For the first evaluation exercise, also described in 4.2, the corresponding argument pattern was instantiated for each of the generic *mechatronic system Partes*. The exercise demonstrated that it is possible to construct a set of claims for each of the generic *mechatronic system Partes* and link them together using common context symbols. However, the instantiation of the argument pattern follows directly from the definition of the ontology, so the result is not surprising and not particularly significant.

For the second evaluation exercise, the argument patterns for a generic *mechatronic system* were instantiated for some of the *Partes*, as presented in Appendix C. The instantiation used material from a previous mechatronic project, 4CAS. Potential issues with the use of the 4CAS example are discussed in 7.6 below. The exercise showed that all the argument contexts and claims could be instantiated with relevant 4CAS related documentation. All of the properties, stated as contexts, that had to be demonstrated were adapted from the corresponding ISO 26262 requirements. The design artefacts, stated as contexts, were instantiated in a number of ways. Sometimes, 4CAS project data was quoted directly, e.g. a named *hazardous event*. Sometimes, a direct reference was made to 4CAS project documentation that is given in Chapter 4. In some instances, reference was made to 4CAS documentation not given in the thesis, e.g. requirements database. For the 4CAS physical parts, a general reference was made. In terms of the GSN, the claims were not developed

further than the level given in the generic argument pattern. The claims were argued at that level in a number of ways. In one instance the type of argument required was discussed but not given. In some instances 4CAS project data was quoted directly. In some instances a reference was made to 4CAS project documentation not given in the thesis, although in some cases it was summarised. In some instances a reference was made to documentation that was not produced by the 4CAS project, although there is no reason why such documentation could not be produced. In some instances reference was made to MISRA guidelines, [189], for suggestions of topics which could be argued over to support the claim. Finally, in some instances reference was made to material produced in other *Pars* as this reflects the structure of the complete argument. The exercise did not reveal the need for documentation or rationale that could not in principle be produced.

Although the evaluation exercise did not reveal any reasons why the argument pattern could not be implemented, it is recognised that this was only a partial evaluation as it only involved three out of the seven *Partes* which define the generic *mechatronic system*. The lack of coverage of the *Pars* 4, *E/E system* design, *Pars* 5, hardware design and *Pars* 6, software design, is not so significant as this is subject to other work by MISRA, [189]. However, the fact that *Pars* 7, mechanical design, was not included represents a significant gap in the evaluation. Although the evaluation was only based on a single *hazardous event*, there is no reason to suppose that other *hazardous events* would reveal unsurmountable difficulties.

Conclusion

We have gone some way towards showing that the *Pars* safety pattern can be used in practice as a means of structuring a mechatronic safety argument. We acknowledge that the argument pattern is only partially evaluated, with the absence of any evaluation of the mechanical *Pars* being particularly serious. We also acknowledge that the *Pars* safety pattern is based on a partially evaluated *Pars* ontology. Nevertheless, the approach shows promise. Further evaluation is discussed in 7.7.1.

Our approach of basing a safety argument on a design pattern, and only arguing over the safety related artefacts and properties, has been shown to work in practice. While it was necessary to define some new safety artefacts specifically for the *mechatronic system*, e.g. the *Mechatronic Functional Safety Concept*, basing them on their equivalents in ISO 26262 meant that this was easily accomplished.

We believe that basing the argument pattern on the ontology is a novel approach. The composition of the different arguments of each *Pars* into an argument for the whole system is not entirely novel, as the concept of modular safety case is well established, [202]. In practice, it will be a management challenge to collate the information from multiple sources and ensure the material is at the correct version and is consistent.

The argument pattern requires that claims for each design artefact be made and supported by evidence. In practice, there may be many design artefacts; documenting and supporting claims for all of them may be impractical, in which case it is necessary to make decisions about which claims to fully document. Such decisions could be informed by the criticality of the safety requirements being implemented, the novelty of the design or the complexity of the design. More guidance on this topic is given the MISRA document, [189].

7.4 TO3: To establish a linkage of integrity to mechanical development

7.4.1 Introduction

As explained in the section on *levels* in 2.3.3, the concept of integrity is key to *E/E system* functional safety standards. In ISO 26262 this is represented by the *ASIL* value. It starts with an assessment of the unmitigated risk which, as we reasoned in section 4.4, is as applicable to a *mechatronic system* as to an *E/E system*. It then translates into the rigour needed to implement the safety requirements necessary to mitigate the assessed unmitigated risk. The degree of rigour[4] applied is then used to justify a claim concerning the integrity of the developed product. This concept is not present in mechanical engineering.

We have decided to use the DFMEA process as a means to establish a link between the assessed unmitigated risk and the integrity required of the mechanical engineering development. To establish this link the following are necessary:

1. The *failure modes* of the DFMEA have to be associated with the relevant *mechatronic technical safety requirements* that would be affected by the *failure mode*
2. For those *failures modes* that are so associated, the integrity of the safety requirement has to be assigned to the *failure mode*
3. The meaning of the integrity, in terms of the choice of *prevention controls* and *detection controls* used to mitigate the *failure mode*, has to be defined

The first of these is achieved by defining the boundary of the DFMEA such that the relationship to the *mechatronic technical safety requirements* is clearly documented. The DFMEA step of determining the *effect* at the boundary, see A.6, will then establish the necessary link.

To achieve the second, we first proposed a means by which the two aspects of the *ASIL* value, risk assessment and required process rigour, could be separated. This is described in sections 6.4 and 6.5. The ISO 26262 risk assessment is applied to a *mechatronic system*, but, instead of the result being assigned a value of *ASIL*, it is assigned a value of unmitigated risk R_{Un}. The value of R_{Un} is assigned to all the safety requirements derived to mitigate the risk. In order to determine the process

[4] It is acknowledged that the integrity of the developed product may also be justified based on design considerations, but we confine ourselves to only process rigout in this discussion.

rigour needed to implement the safety requirements, the value of R_{Un} is mapped to two other values. One is an *ASIL* value which indicates the requirements from ISO 26262 that are applicable to the *Mechatronic Item Definition & HARA* (including mechatronic safety goals), the *Mechatronic Functional Safety Concept*, the *Mechatronic Technical Safety Concept*, the *E/E Technical Safety Concept*, the hardware development and the software development. The other is a SS_{SC} value which becomes associated with the DFMEA *failure modes* via the effect at the boundary, as described above. The flow of values of R_{Un}, *ASIL* and SS_{SC} across the mechatronic *Partes* is shown in Figure 77. These proposals, while having a degree of face validity, have not been subject to any evaluation exercises. The topic of evaluation is discussed in 7.7.2.

Defining the meaning of the integrity in terms of the choice of prevention and detection controls is discussed below in 7.7.3, but we first discuss the topic of *special characteristics* upon which the concept of SS_{SC} values is based.

7.4.2 The Use of Special Characteristics

The proposal is to use the new concept of SS_{SC} values to feed the concept of integrity into the development of mechanical components via the DFMEA, as described above. Our intention is to use mechanisms that are already accepted practice rather than proposing something entirely new. The introduction of something new may well meet with resistance and would take longer for it to become accepted practice. The use of *special characteristics* is already established practice in the automotive industry and is required by IATF 16949:2016, [143], which defines them as "*those characteristics of the design that are crucial to the safe and proper functioning of the product*". So, while the normal process is for the DFMEA to determine the special characteristics, our proposed alternative usage, as a means to feed safety-related information, is consistent with the spirit of the standard. IATF 16949:2016 is universally used in the automotive industry and certification by external auditors is usually obtained. If our proposal was accepted, and this usage was in the scope of the external audit, it would then become institutionalised within organisations.

7.4.3 Defining Integrity in the Mechanical Process

We mentioned in Chapter 6 the daunting challenge of introducing the concept of integrity into the mechanical design process which requires the calibration of the SS_{SC} values. The mechanical domain itself embraces a range of different technologies, e.g. pneumatic, hydraulic. Each of these have their own body of theory and practice as defined in standards and text books. The use of the DFMEA technique is likely to be adapted to the particular technology, and likewise the design controls used maybe technology-specific. By taking a very general approach we have abstracted the scheme from this challenge, but the challenge still remains. While some potential approaches to defining the meaning of *special characteristics* were described in Chapter 6 we recognise that

these are only theoretical and have not been subject to any evaluation. An evaluation of this topic is beyond the scope of that typical for a doctoral thesis.

The use of *special characteristics*, as presented in Chapter 6, is not current practice and is an alien concept for mechanical engineering. From the second case study, Appendix D, it was seen that the current practice is to always follow one process, so having to define five variations of process would be a major challenge. However, functional safety standards and guidelines are application-neutral, and try to give guidance for any application within their unmitigated risk range results in them specifying different requirements depending on the assessment of the unmitigated risk, e.g. ASILA – ASILD. In practice, organisational units often develop only a narrow range of products that all tend to fall within the same place on the unmitigated risk scale. So, they have a single process that is carried out for all developments. The role of achieving the integrity requirements only occurs when the process is first defined and then when it is updated as industry practice develops. This is less true for a large organisation that produces electronic control units and may, within it, produce products for a range of values on the unmitigated risk scale and have a generic company process that is used for all products. However, even within the large company, there will be divisions and departments that specialise in a narrow range of products on the unmitigated risk scale, especially for products at the higher end of the unmitigated risk scale. In such large organisations it is customary for the generic process to be tailored for the particular products. It is also the case that departments and divisions specialise in particular mechanical products, especially in the high end of the unmitigated risk scale. So, the number of *special characteristics* to be defined, and the process variations that go with them, will be reduced.

For an *E/E system*¸ when a supplier declares that its component has been developed according to ISO 26262 for a particular value of *ASIL*, there is a common understanding in the industry of what this implies. This understanding is essential for the body that is responsible for integrating components from different suppliers, be they hardware or software. Such an understanding greatly aids the construction of the overall safety argument. An industry benchmark for *special characteristics* that can play a similar role for the mechanical components is necessary in order to ensure that a mechanical assembly is created from components which have an integrity consistent with that dictated by the assessed unmitigated risk and the design of the system. The need to have consistency of integrity between the mechanical components and the E/E control is becoming more important with the trend for the primary actuation of the vehicle to be allocated to smart actuators which then respond to actuation requests produced by centralised vehicle controllers.

The calibration of the SS_{SC} values is discussed further in 7.7.2.

7.4.4 Conditional Probability Risk Model

Given the proposed use of the DFMEA as the link to mechanical development, there is a need to understand the relationship between the risk assessment it performs and the risk assessment that is required by the ISO 26262 standard. This understanding was gained by drawing a bow-tie diagram, Figure 76: Fault to harm model, and the creation of the conditional probability model based on it. As the ISO 26262 approach was based on the assumption that the *hazard* had occurred, the use of conditional probability was the obvious way to model this.

The conditional probability model defined a number of terms:

- *fault* – the potential cause of *faulty-machine-behaviour*
- P_{fault} – the probability that the *fault* will occur
- *P[faulty-machine-behaviour | fault]* – the probability that the *fault* will result in *faulty-machine-behaviour*
- *faulty-machine-behaviour* – associated with a *hazard*
- P_{harm} – the probability that *harm* will occur as a result of the *hazard*
- *P[harm | faulty-machine-behaviour]* – that the *faulty-machine-behaviour* will result in *harm*

In this model, the DFMEA assesses P_{fault} * *P[faulty-machine-behaviour | fault]*. In DFMEA terms, the *fault* equates to the *failure mode*. It then employs *prevention controls* and *detection controls* to reduce P_{fault} to an acceptable value.

The ISO 26262 risk assessment scheme assumes that the *faulty-machine-behaviour/hazard* has occurred and assesses *P[harm | faulty-machine-behaviour]*. In ISO 26262, the value of P_{fault} is more closely associated with the integrity levels; by meeting the standard's requirements for the *ASIL* value, it may be claimed that the value of P_{fault}, due to systematic and random causes, is sufficiently low. So, for ISO 26262, *P[harm | faulty-machine-behaviour]* is assessed and used to determine the integrity necessary to claim that the value of P_{fault} is sufficiently low.

It is not unknown for conditional probability to be used as part of an FMEA. In a quantitative evaluation of an FMEA, a beta factor is used to represent the conditional probability that the failure effect will result in the identified severity classification, given that the failure mode occurs, [203]. This is effectively *P[harm | faulty-machine-behaviour]* in our model. Interestingly, the value of the beta factor is determined by the analyst's best judgment as to the likelihood that the loss will occur.

The model has proved useful in understanding the relationship between the different assessments of the DFMEA and the ISO 26262 risk assessment. It has allowed us to build a bridge between the two by the use of the SS_{SC} values. While with any model it is possible to find examples that do not quite fit, nevertheless the model seems to provide a broad understanding of the difference between

what the two risk assessments are trying to achieve. The model, while having a degree of face validity, has not been subject to any evaluation exercises.

7.5 TO4: To establish evidence for claims for mechanical development

A safety argument needs to be supported by evidence. For the *mechatronic system* safety argument most of the evidence required can be taken from ISO 26262. This can be as a reinterpretation of the *E/E system* requirements as is the case for the M*echatronic Item Definition & HARA*, the *Mechatronic Functional Safety Concept*, the *Mechatronic Technical Safety Concept*, and the *E/E Technical Safety Concept*. In the case of hardware development and software development, the evidence required can be taken directly from ISO 26262. However, the question arises as to where the evidence to support claims regarding the mechanical development can be taken from.

There are two types of evidence: that related to the design argument claims and that related to the safety argument claims. As noted when discussing properties of the mechanical design in section 4.2.7, specific design properties are not given in the literature, only broad topics for evaluation from which it may be possible to derive specific properties that could be reasoned about in the argument. This topic of possible mechanical design properties is not expanded further, but is an area that could benefit from further research. As our objective is to develop a safety argument, the absence of detail concerning evidence to support the mechanical design argument is not an issue, i.e. we are only interested in arguing over the safety requirements. This is also the case for the *E/E system* design argument.

Regarding evidence to support safety argument claims, we noted when discussing properties of the mechanical components in section 7.4.2, that testing is part of the mechanical design process. The testing objectives, means and results for design artefacts could be used to support *satisfaction* claims. Specific details have not been elucidated, but the mechanical design evaluation topics, Table 11 and Table 12, provide a starting point for determining the relevant properties of the physical components. Also, noted in 4.2.7, fulfilment of cascaded requirements is a key physical realisation property; this includes safety requirements. This fulfilment would be a claim in the argument, and the evidence for this could be established by the use of test techniques in a similar way as for the *E/E system*. One of the key claims of the safety argument is that, for mechanical causes of malfunctioning behaviour, a complete set of safety requirements have been identified and put in place to sufficiently mitigate the causes and/or effects of malfunctioning behaviour.

We have proposed a scheme by which mechanical safety requirements can be related to the mechatronic risk assessment, 7.4.1. In doing so, the mechanical safety requirements can have an assigned value of integrity, SS_{SC} values, related to the risk assessment. The link to the mechanical safety requirements is via the DFMEA process, which then has to identify *prevention controls* and

detection controls which are commensurate with the integrity, based on the calibration of the SS_{SC} values. In terms of a safety argument, this process has to support a claim of the form "*Failures of mechanical components that violate mechatronic technical safety requirements have been mitigated by prevention and detection controls*". To support the claim, the process needs to have run and produced the design documentation. But evidence is also required for supporting claims regarding how well the process has been performed. These claims are examples of the MISRA *means* and *organisational environment* claims, [187]. This raises the question of whether the DFMEA process has the potential to support such claims.

Research Method

To determine if the DFMEA process has the potential to support *means* and *organisational environment* claims, a case study was conducted. The purpose of this was to understand the extent to which the DFMEA as practised does, or could, produce the evidence necessary to support claims related to the mechanical development. It addressed the research question, "*What is the established role and practice of using DFMEA in an automotive context and the factors that influence its judged effectiveness?*"

Conclusion

The case study is reported in Chapter 5. The conclusions from the study were that the DFMEA does have the potential to provide evidence to support safety claims concerning mechanical components. The safety requirements necessary for the claims related to the mitigation of the causes and/or effects of malfunctioning behaviour are captured in the *prevention controls* and *detection controls*. The study also highlighted themes that could be used to support claims related to the rigour with which the DFMEA had been performed. This is related to the concept of integrity, as mentioned above. One of these themes is the governance of the DFMEA process, and the study highlighted this as a potential weakness, 5.3.4. This topic and further evaluation are discussed in 7.7.1.

7.6 Use of Four Corner Air Suspension for Evaluation Exercises

The *Four Corner Air Suspension* system was used for three evaluation exercises:

- Case study 2 looking at the practicality dividing a system into a set of *Partes*
- An example of instantiating a set of *Partes* for a *mechatronic system*
- An example of instantiating the safety argument pattern for a set of *Partes* for a *mechatronic system*

There are a number of reasons why the 4CAS system was used for these exercises. The system is an in-house development which means that far more is known about the development than if a supplier had been responsible for delivering it. Although not published at the time of the development, the concepts which ISO 26262 contains were applied to the development of the

system which means that material we wished to use was available. It was also used as a case study for the DTi MOSAIC project, [186], which meant that more documentation was produced than would otherwise have been the case. It has been in production since 2004 and the material used in the evaluations is already in the public domain. The system is well-known to the author, and many of the staff who originally worked on it are still available to be interviewed. The system has the classic characteristics of a *mechatronic system*, in that it is the electronic software based control of a hydraulic system to achieve mechanical affects at the vehicle level.

However, there are limitations in the repeated use of the same system for the different evaluation exercises. It represents only one particular system with one type of actuation. The range of automotive actuation is much broader than an hydraulic system and includes control via pneumatic systems, electric motors and also the generation of light and sound. Also, this is not typical of the majority of the systems produced by an OEM, and historically the suppliers have not been willing to reveal all their internal information; this would hinder the practical use of this approach.

Much of the design documentation was already congruent with the proposed approach. While this was seen as an advantage for completing the evaluation exercises it also makes the results less representative of systems in general.

7.7 Further Evaluation

To achieve the thesis objectives stated in 7.1, a number of proposals have been made. These have all been subject to a partial evaluation. In this section we discuss the possibilities for further evaluation. The proposals are made regarding:

- The *Pars* approach based on a design ontology and a safety argument pattern
- The use of *special characteristics* to communicate integrity into mechanical development process via the DFMEA process
- The use of *special characteristics* to calibrate the mechanical development process according to the integrity communicated
- The use of the DFMEA to provide supporting evidence for the safety argument

These proposals are discussed under the headings of:

- The *Pars* approach
- Use of *Special Characteristics*
- Use of the DFMEA

Additional comments are also made concerning All Product Lifecycle Stages, 7.7.4.

7.7.1 The *Pars* approach

To fully evaluate the *Pars* approach it is necessary to plan a development with the intention of producing all the relevant documentation indicated by the *Partes* ontologies for each abstraction level. The extent to which this is practical depends on whether the exercise is being carried out by an OEM or a supplier. It would be beneficial for evaluation to be performed by both OEMs and suppliers as both types of organisation are necessarily involved in the development of the complete system. In both cases the evaluation scope needs to take into account all the parties, both within the organisation and external to it, who have to produce or receive the information. ISO 26262 already has the requirement for a *distributed interface agreement* to be drawn up between different organisations. The evaluation should investigate how this needs to be structured to accommodate the information exchange necessary for the *Pars* approach, especially for the supplier of mechanical components, for whom this would be a new way of working. To fully evaluate all aspects of the approach the development process would be based on the generic *Pars* process which has not been subject to any evaluation in this thesis.

It would be beneficial to apply the approach to something other than a chassis system, e.g. a powertrain, driveline or body system. This would shed light on how widely applicable the approach is. The *Partes* division presented in this thesis need not necessarily be used as the division will be strongly influenced by the nature of the system and the organisation developing the system. However, it is recommended that the *Pars* defined for the *Mechatronic Item Definition and the Hazard Analysis and Risk Assessment* and *Mechatronic Functional Safety Concept* be used. These have been defined in such a way as to be consistent with the MISRA framework, [189], and this is key to our overall approach. It is important that the mechanical development *Pars* is included in the case study as the evaluation of the ontology and argument for this *Pars* is particularly weak.

Further investigations into the applicability of the *Pars* approach to mechanical development would involve: identifying specific properties of design artefacts for a given development process; determining if it is possible to derive claims related to these properties in terms of the MISRA themes of *rationale*, *means* and *satisfaction*, [187]; and determining if the necessary supporting evidence could be identified. These properties could be for design and safety, but it is safety which we are interested in for the safety argument. One example is testing objectives, methods and results for mechanical components.

The scope of this thesis does not include any consideration of the governance of the overall process. To fully understand the practicality of the approach it is necessary to investigate the impact of the *Pars* approach on the requirements for project planning, project management and overall process control, as stated in the quality and safety standards. This could be as part of the wider study

discussed above. The impact may not be large, as the *Pars* approach is already based on the current practice, but it may inform the requirements for managing the interfaces between organisations.

7.7.2 Use of *Special Characteristics*

There are two aspects to our proposed use of *special characteristics*:

- Linking integrity into mechanical development process via the DFMEA process
- Calibrating the mechanical development process according to the required integrity

A flowchart showing the proposal for linking the mechatronic risk assessment to the DFMEA process is shown in Figure 78. This allows the DFMEA *failure modes* to be related to the integrity values produced by the risk assessment. For a full evaluation, a trial of this complete process is needed, with the necessary changes made to the ISO 26262 based risk assessment and to the DFMEA process.

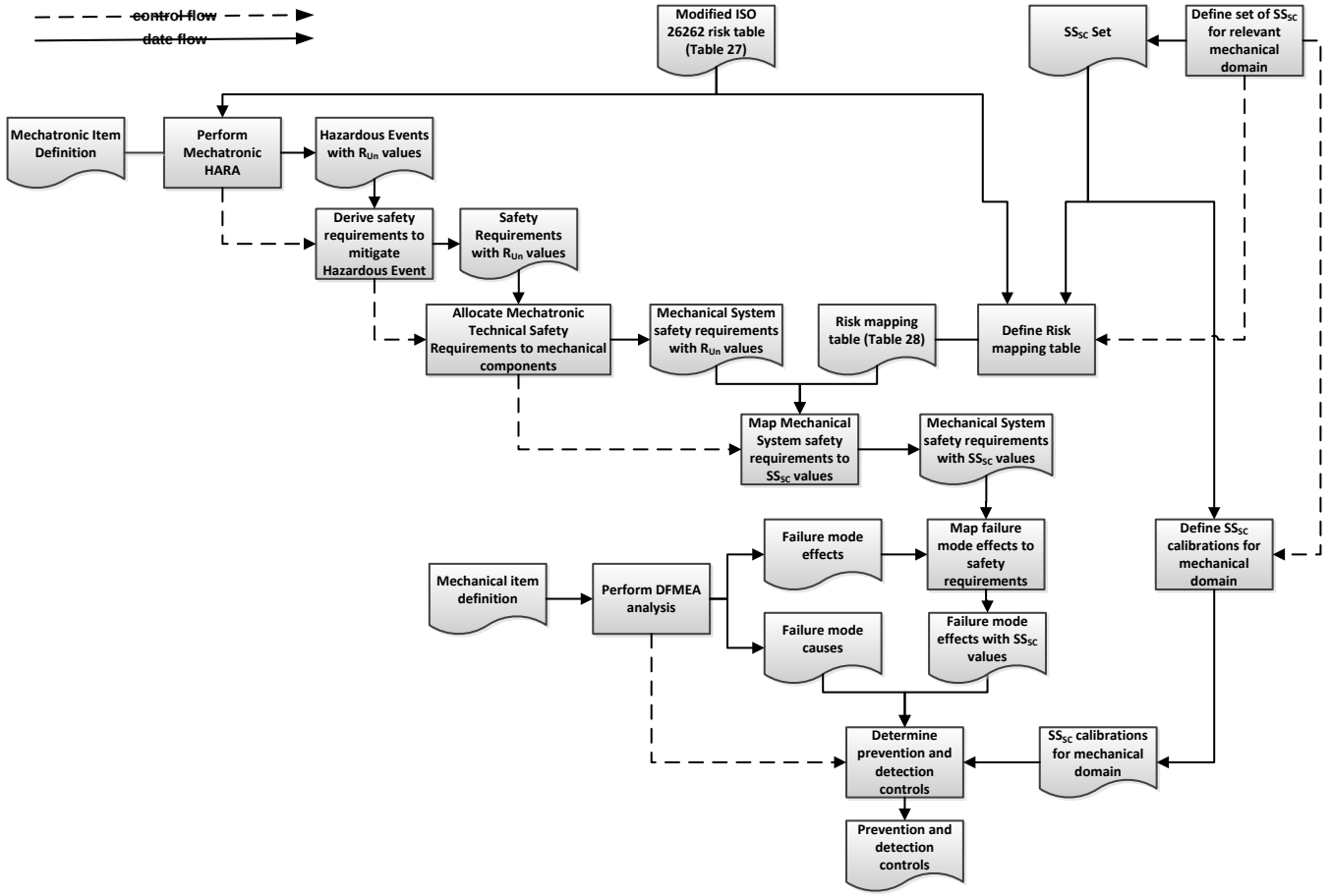

Figure 78: Risk Assessment and DFMEA process

The use of *special characteristics* is essential for the practical use of our approach. While some potential approaches to defining the meaning of *special characteristics* were described in Chapter 6, we recognise that these are only theoretical and have not been subject to any evaluation. There are two areas that need to be investigated. One is the willingness of the quality process staff to accept that integrity should be included in their considerations; this would be a break from many years of established practice. The other is the feasibility of defining different process variations for different *special characteristics*. It is not intended that mechanical development should adopt the ISO 26262 approach, where the majority of the development process is dictated by allocated integrity values.

A full evaluation should cover a number of different organisations using different technologies which have control by an *E/E system*. Each organisation would define a number of *special characteristics* as appropriate for their technology and based on their current practice. For those that produced a range of products with different values of unmitigated risk, the different definitions of the *special characteristics* would be checked against the rigour of process for the *E/E system* based on the *ASIL* value. The results of the studies in the different organisations would then be compared to see if there was consistency and the reasons for any inconsistencies investigated. Ideally, a metrification framework would be defined to allow an objective evaluation. In doing this, the definition of the *special characteristics* would effectively be given a calibration. This calibration would have to be established over a period of time by feeding back actual experience into the process. Therefore, the study would need to be repeated after a period of time to continue to ensure consistency. Establishing a benchmark may take many studies over many years, as the calibration process, based on field experience, converges to some generally agreed position. Once such a position is established, the possibility of an international standard becomes a possibility.

7.7.3 Use of the DFMEA

While the conclusions from the study were positive, the limitations of the scope of the study, which focused on depth rather than breadth, have to be recognised. While the case study was conducted in a major global automotive OEM whose approach is not unrepresentative of the industry in general, it is still only a single company. Further longitudinal studies involving other OEMs and tier 1 suppliers are necessary for the conclusions to be generalised with confidence. Also, the study had a limited number of 16 participants; the roles were biased towards the DFMEA experts rather than the practitioners, and the coverage of the engineering disciplines was not uniform, see Table 13 and Table 14. Future studies should involve a greater number of non-specialists in the exercise and should correct the author's error in question Q3.2 as mentioned in 5.3.3.

We mentioned in 5.5 that it would be interesting to understand if the use of the DFMEA would benefit from having an assurance argument, the rationale being that a more structured way to record the results and the reasoning would help as systems become more complex due to the addition of *E/E system* control. An assurance argument for the use of the DFMEA as a quality measure could start with a top claim of the form, "*All failure mode of the {item} have been identified and sufficiently mitigated"*. An investigation into the development of these claims using the material from the case study performed here, or other case studies, would provide insight into the benefits of such an approach. By way of contrast, the assurance argument we require for the use of a DFMEA in a safety context could start with a top claim of the form, "*All failure modes of the {item} related to hazardous events of {mechatronic item} have been identified and mitigated with an integrity commensurate with the assessed risk of the hazardous events*". This claim would involve the use of the SS_{SC} values.

7.7.4 All Product Lifecycle Stages

The scope of this thesis does not include the update and maintenance of the safety argument during the stages of the *mechatronic system*'s lifecycle other than that of development. The maintenance of the safety argument during other lifecycle stages, such as operation, modification and decommissioning, is equally important to the overall safety record of the system. The impact of considering other lifecycle stages will include: change control and configuration management, governance, the identification of new hazards, the reassessment of the unmitigated risk, and the addition and/or modification of safety requirements. The integrity values of the safety requirements may also be affected. A study into these aspects could only be conducted once the basic *Pars* approach has been established within the product development process of an organisation.

7.8 Summary of Evaluation

In Chapter 1, the thesis hypothesis was stated as, "*A risk-based safety argument for a complete mechatronic system can be constructed that enables the explicit and systematic derivation of safety requirements, with assigned integrity values, and that utilises evidence already produced by the established development practices for E/E systems and mechanical components*. Based on this, the research objective was stated as, "*To establish a uniform approach to justifying that an automotive mechatronic system is fit to be put into production from a "functional safety" perspective"*. From this, four thesis objectives were derived:

- TO1: To establish a design representation upon which a safety argument can be based
- TO2: To establish a safety argument pattern based on the design representation
- TO3: To establish a linkage of functional safety integrity to mechanical development
- TO4: To establish a means of providing evidence to support claims related to mechanical development

In pursuing these thesis objectives the following contributions have been presented:

1. A *model-based approach* to representing the different divisions of work necessary to create a multi-technology system, that honours the co-evolution of safety requirements, and which provides the basis for a complete risk-based safety argument for a *mechatronic system*
2. A case study on the practical application of DFMEA in an automotive OEM which assesses the extent to which, as practised, it does, or could, produce the evidence necessary to support the mechatronic system safety argument
3. The creation of a *mechatronic system* safety argument pattern, and its evaluation, by the application of the *model-based approach*

Table 33 relates the contributions to the thesis objectives.

Thesis Objective		Contribution 1	Contribution 2	Contribution 3
TO1	To establish a design representation			
TO2	To establish a safety argument pattern			
TO3	To establish a linkage of functional safety integrity to mechanical development			
TO4	To establish a means of providing evidence to support claims related to mechanical development			

Table 33: Sub-objectives and Contributions

Contribution 1 is the creation of two frameworks; one for deriving safety requirements and the other for a mechatronic safety argument pattern, as presented in Chapter 3 and in Chapter 4. The evaluation of these frameworks, reported in sections 7.2 and 7.3, showed that the overall result is positive. The participants were able to engage with the material and the view was expressed that it is an improvement over current practice. There were some practical concerns about the availability of the documents, especially from suppliers, and the need express the interplay between the different development streams in a way that represents actual practice. Assent was forthcoming by both those involved with *E/E system* design and those involved with mechanical design.

Contribution 2 is the assessment of the established use of the DFMEA process for mechanical components by means of a case study and is presented in Chapter 5. The conclusions from the study, 7.5, are that the DFMEA does have the potential to provide the evidence to support a safety argument, but, for this potential to be realised, strong governance is required to ensure that it is performed fully and with sufficient rigour.

Contribution 3 is a means of assigning integrity values to safety requirements cascaded to mechanical components and is presented in Chapter 6. Its evaluation is discussed in section 7.4. There are number of different aspects to this which we consider in turn.

We have based the safety argument pattern on the generic design ontology of the *Pars* and then composed the overall system safety argument from the individual *Pars* arguments. While this has not been formally evaluated, there is already a precedent for a compositional approach set by the

work on modular safety cases, [202]. Structuring the safety argument around the cascade of safety requirements also has precedent set by the MISRA work, [200], [187]. A partial example of the instantiation of the mechatronic safety argument pattern, based on the 4CAS system, is given in Appendix C.

The conditional probability risk model has no evaluation, but as presented in Chapter 6 using the bow-tie diagram, it has an element of face-validity.

The use of *special characteristics* as a means to feed the concept of integrity into the mechanical process is a key aspect of the scheme but in need of a proper evaluation, as described in section 7.5. There are two aspects that need to be established. One is whether it will be accepted by the industry; there is a rationale for its use, but opinion of the industry has not been tested. The other is the practical matter of defining meanings for the *special characteristics* such that they do provide the valid assurance of integrity required by the overall safety argument.

Chapter 8 Conclusion and Future Work

8.1 Thesis Summary and Contributions

This thesis has defined and evaluated a model-based assurance approach for constructing a safety argument for a *mechatronic system*. Establishing this assurance approach entailed producing a common means of representing the different parts of the system that may be the responsibility of different departments. It also entailed showing how these representations could be applied to a *mechatronic system* to produce a hierarchy of design which extended the requirements based on ISO 26262.

To arrive at the model-based assurance approach a number of challenges had to be met. The first was finding an underlying uniform design model able to include both the mechanical and E/E aspects of a *mechatronic system*. Given this uniform design model, we had to understand how it could be used as the basis for the safety argument. We then had to see how well the design model and safety argument pattern would generalise to a *mechatronic system*. In applying it to a *mechatronic system* we had to consider the safety lifecycle for a mechatronic system and the new safety documentation that it would require. We also had to consider what mechanical design artefacts could be available as evidence to support the argument and the potential of the DFMEA to provide supporting evidence for the safety argument. To make use of the results of the DFMEA, we had to understand the relationship between the assessed unmitigated risk, determined by the ISO 26262 scheme, and the DFMEA risk assessment of component failure modes. From this we had to propose a means of conveying the integrity value, associated with safety requirements allocated to the mechanical system, which is derived from the unmitigated risk assessment. Lastly, we were faced with the challenge of giving an interpretation of integrity in the mechanical design process.

The resultant model-based assurance approach provides a means for safety requirements, with integrity values, to be fed into the mechanical design, and for the integrity requirements to be integrated into the commonly used DFMEA process. In this thesis we have focused on three main areas of contribution, namely:

1. A *model-based approach* to representing the different divisions of work necessary to create a multi-technology system that honours the co-evolution of safety requirements, and which provides the basis for a complete risk-based safety argument for a *mechatronic system*
2. A case study on the practical application of DFMEA in an automotive OEM which assesses the extent to which, as practised, it does, or could, produce the evidence necessary to support the *mechatronic system* safety argument
3. The creation of a *mechatronic system* safety argument pattern, and its evaluation, by the application of the *model-based approach*

There is much more to the development of a *mechatronic system* than what has been discussed in this thesis. As mentioned in Chapter 1, the overall development process is out of scope, as is the governance of the process, overall, and at each stage. Also, the scope only includes the safety argument and not the whole safety case.

It should also be noted that it is current practice to develop a *mechanical system* under *E/E system* control as a *mechatronic system*, but this is achieved informally rather than with defined mechatronics documents. For example, the introduction to ISO 26262 acknowledges the increasing growth of *mechatronic systems*, but then limits its scope to the *E/E system*. Here we have made the case for a *mechatronic safety argument*, which then necessitates the creation of mechatronic documents.

8.1.1 The division of the engineering process into Partes

In Chapter 3, starting from the existing material on systems engineering, analysis techniques and argument patterns, we derived a novel representation, *Pars*, for a division of the product engineering task. A *Pars* is defined by a generic ontology and has an accompanying design argument pattern based on the ontology. A generic process description for a *Pars* has also been presented. We showed how an *E/E system*, developed according to ISO 26262, could be divided into a set of *Partes*, and how the requirements and work products of the standard related to the generic ontology and safety argument pattern of each *Pars*.

While the commonly used diagrammatic representations of system development, e.g. Figure 1, Figure 4 and Figure 8, cannot be used to derive generic system structures that can be used as the basis of a safety argument pattern, they do provide a clear impression of the overall structure and process. With the division into *Partes*, this *big picture* view is not so apparent, and we have not provided an equivalent to these figures. This point was made by one of the participants in the second case study.

We highlighted in section 3.3.1 that the *Pars* approach is still open to composition issues and could only offer the rigorous use of change control and configuration management as a solution. These are topics that are not within the scope of this thesis.

While the intention is that a *Pars* can be defined based on any arbitrary division of the work, the evaluation has only been for one system in the narrow context of a *mechatronic system* aligned closely with ISO 26262.

8.1.2 The application of Pars division approach to a mechatronic system

In Chapter 4 we presented the application of the *Pars* approach to a *mechatronic system*. This required the division of the *mechatronic system* into a set of *Partes* and the definition of some new

safety design artefacts. The division was illustrated using actual design artefacts from a previously developed *Four Corner Air Suspension* system (4CAS). This division was the subject of a case study, presented in Chapter 7, involving the engineers who were involved in the original 4CAS development. The results show that the case study participants considered that the taking of a mechatronic perspective was an improvement over current practice and could relate their activities and the design artefacts to the division into *Pars*. It was noted that the division between the *mechatronic Pars* and the *mechanical Pars* was somewhat artificial as the work involved the same staff co-evolving both aspects at the same time.

In order to apply the generic model to the mechanical *Pars*, it was necessary to recast the generic design artefacts as mechanical design artefacts. There is no mechanical standard process model equivalent to the standard software lifecycle for describing development, e.g. V-model, waterfall model, spiral model, [204]. In the absence of a standard model we used a model from a standard text book, [48]. In practice, the recasting of the mechanical *Pars* would have to be based on the proprietary process of each organisation. However, the safety artefacts identified are sufficient for our purpose of a safety argument.

The evaluation of the *Partes* division report in Chapter 8 was based on only one system, 4CAS. This is an in-house development, which is not typical, and the application of the approach to the more usual *tier 1 supplier*-led development has not been evaluated.

8.1.3 Practical Application of DFMEA Case Study

In Chapter 5 we presented a case study into the industrial practice for the use of the DFMEA on mechanical components. This showed that the DFMEA process has the potential to provide the evidence required to support a safety argument. It also highlighted the need for strong governance over the enactment of the process. However, the issue of governance is not within the scope of this thesis, so there remains some practical considerations that have not been addressed.

We also questioned whether the DFMEA quality process would benefit from having an assurance case structure, as not everything can be dealt with by strong governance. The case study did reveal a degree of variety in how a DFMEA is performed and gives the impression that current practice may be being stretched to the limit of its capability. As systems are becoming more complex, especially with the addition of *E/E system* control, there may well be some benefit to be gained by having a more structured way to record results and reasoning.

8.1.4 An approach to creating a safety argument for a mechatronic system

In Chapter 6 we showed a means of separating out the two meanings of the ISO 26262 term *ASIL*, which are: an indication of the assessed unmitigated risk, and the integrity with which safety requirements are to be implemented. This was based on a conditional probability risk model and

was necessary to allow the concept of integrity to be fed into the mechanical design. We then showed that *special characteristics* could be used as a means to feed integrity values into a DFMEA quality-based process used in mechanical engineering. We note that, even for a *mechatronic system*, it is still possible to assign safety requirements to *external measures* which can still include non-E/E technology. For these to have an assigned integrity value would require the widespread adoption of the proposed use of *special characteristics*.

We acknowledge that the proposed use of *special characteristics* as a means of feeding the concept of integrity into a DFMEA quality-based process used in mechanical engineering has had no evaluation.

The construction of a complete safety argument for a *mechatronic system* divided into a set of *Pars* requires strong governance of the whole process, as any misuse would undermine the integrity of the whole safety argument. This aspect of governance is outside the scope of this thesis.

8.2 Recommendations

In 7.7 we presented ideas for further evaluation of the work reported in this thesis. In this section we make recommendations for the next steps.

8.2.1 The *Pars* Approach

A *mechatronic system* other than a chassis system should be evaluated and the scope kept to something practical. While it is not essential to use the *Partes* for the generic *mechatronic system* that are defined in this thesis, it is recommended that the *Pars* defined for the *Mechatronic Item Definition and the Hazard Analysis and Risk Assessment* and *Mechatronic Functional Safety Concept* be used. The other *Partes* could be changed as is appropriate, given the nature of the system and the organisation developing the system. Not every aspect of the *mechatronic system* need be included, but a *Pars* covering some mechanical development should be included. The aim should be to have a slice of ontology and argument from the risk assessment to the mechanical safety requirements. It is important to ensure that all participants, both within the organisation and externally, are willing to take part in the information exchange.

Of particular interest is the applicability of the *Pars* approach to mechanical development. It is recommended that an exercise be performed to identify specific properties of design artefacts that could be used to support the instantiation of the mechanical *Pars* safety argument. To fully evaluate the *Pars* approach on the mechanical development, it is necessary to define a set of SS_{SC} values with their corresponding process requirements. If a formal set of SS_{SC} values has not been created, it is still possible to trial the approach using a nominal set defined just for that purpose.

For a full evaluation of the *Pars* approach, the exercise would include the governance of the overall process including the impact on project planning and project management. This is only possible once the *Pars* approach is well established in the organisation.

8.2.2 Use of Special Characteristics

It is recommended that the definition of a set of SS_{SC} values, with their corresponding process requirements, first be trialled within a single organisation to assess the practicality and difficulty of the approach. If the attempt is successful, and thought to add value, then a wider trial would have to involve several companies in a cross industry collaborative project.

To trial the linking of the risk assessment to the mechanical safety requirements it is recommended that the process given in Figure 78 be followed to establish the practicality of the proposed scheme. A prerequisite for this is to define a set of SS_{SC} values with their corresponding process requirements. If this has not been done, then it is recommended that a nominal set is defined just for the purpose of the trial.

8.2.3 DFMEA Usage

As described in 7.7.3, it is recommended that further longitudinal studies involving other OEMs and tier 1 suppliers be conducted involving a greater number of non-specialists.

Although not central to this thesis, it is recommended that the use of an assurance argument to provide a rationale for the result of a DFMEA be investigated. As suggested, for the use of the DFMEA as a quality measure, the assurance argument could start with a top claim of the form, "*All failure modes of the {item} have been identified and sufficiently mitigated"*. It is envisaged that the development of the argument would result in claims arguing over the types of topics identified by the case study performed as part of this thesis.

8.3 Concluding Remarks

The disciplines of mechanical engineering and *E/E systems* have developed separately despite being intimately connected. The literature on *mechatronic systems* is concerned with the interface between the two technologies and how to achieve the overall desired performance. Its scope does not include the already established practices for the implementation of the different technologies. This means that there is a lack of the holistic approach necessary for a convincing safety argument for the *mechatronic system*. While the lack of such a holistic approach may not have had a serious impact on the deployment of *mechatronic systems* to date, as has been noted, the systems are becoming more complex and are being used more and more for safety-related applications. The question arises of whether current practice will be sufficient, going forward. This thesis has laid some of the foundations for a holistic approach that are necessary for a complete safety argument

of a *mechatronic system*. The generic nature of the *Pars* approach means it may have the potential for wider application, but this is yet to be established.

Appendix A DFMEA Exposition

A.1 Origins of Failure Mode Effects Analysis

The first standard for *Failure Mode Effects Analysis* (FMEA) was issued in 1949 by the US Armed Forces, MIL P 1629 Procedures for Performing a Failure Mode, Effects and Criticality Analysis, [205]. Over the course of the next three decades other industrial sectors adopted the use of FMEA. These included NASA in 1963, [174], and civil aircraft design in 1967, [206]. The Ford Motor Company started to use FMEA in the late 1970s, [207], as did many other automotive companies. In 1994, SAE published J1739, [208], which was jointly developed by Chrysler Corporation, Ford Motor Company and General Motors Corporation. The most recent edition of this was published in 2009, [159]. The use of J1739 was required by QS9000, [142], which until 2006, was widely used as the automotive version of ISO 9000. In 2006 QS9000 was replaced by ISO/TS 16949, [138], which also requires the use of J1739. In 2016 ISO withdrew TS 16949 but it continues to be published by IATF (International Automotive Task Force) as IATF 16949:2016, [143], and it remains the universally used quality standard in the automotive industry. Other FMEA standards are also published, for example the one by VDA, [172], used widely in the automotive industry, and IEC 60812, [160].

All of the FMEA standards mentioned above describe the process in a number of steps and these are common to all descriptions of the technique, for example one book, [209], describes performing an FMEA in 10 steps, see Table 34.

Step	Description
1	Review the Process or Product
2	Brainstorm Potential failure Modes
3	List Potential Effects for Each Failure Mode
4	Assign a Severity Ranking for each Effect
5	Assign an Occurrence Ranking for each Failure Mode
6	Assign a Detection Ranking for each Failure Mode
7	Calculate the Risk Priority Number for each Failure Mode
8	Prioritise the Failure Modes for action
9	Take action to eliminate or reduce the high-risk Failure Modes
10	Calculate the resulting RPN as the failure modes are reduced

Table 34: 10 Steps of FMEA [209]

A.2 Types of FMEA

The FMEA technique can be used to analyse different types of artefact, e.g. a system concept, a design, a manufacturing process. This gives rise to commonly used terms of *Concept FMEA* (CFMEA), *Design FMEA* (DFMEA) and Process *FMEA* (PFMEA), [210]. The use of the FMEA technique to analyse *software* is also widespread. The description given here applies equally to the CFMEA and the DFMEA.

The 1980 version of Mil 1629, [13], is structured around two tasks. *Task 101* is referred to as an FMEA and its purpose is "*to study the results or effects of item failure on system operation and, to*

classify each potential failure according to its severity". *Task 102* is referred to as *Criticality Analysis* and its purpose is "*to rank each potential failure mode identified in the FMEA Task, according to the combined influence of severity classification and its probability of occurrence based upon the best available data*". The combination of both tasks is often referred to as *Failure Mode Effects and Criticality Analysis* (FMECA) but is also very common for the term FMEA to be used even though the criticality analysis is also being performed.

A.3 FMEA Terms

A number of commons terms are used in the literature on FMEA, these and the relationships between them, are shown in Figure 79 as a SysML Block Diagram.

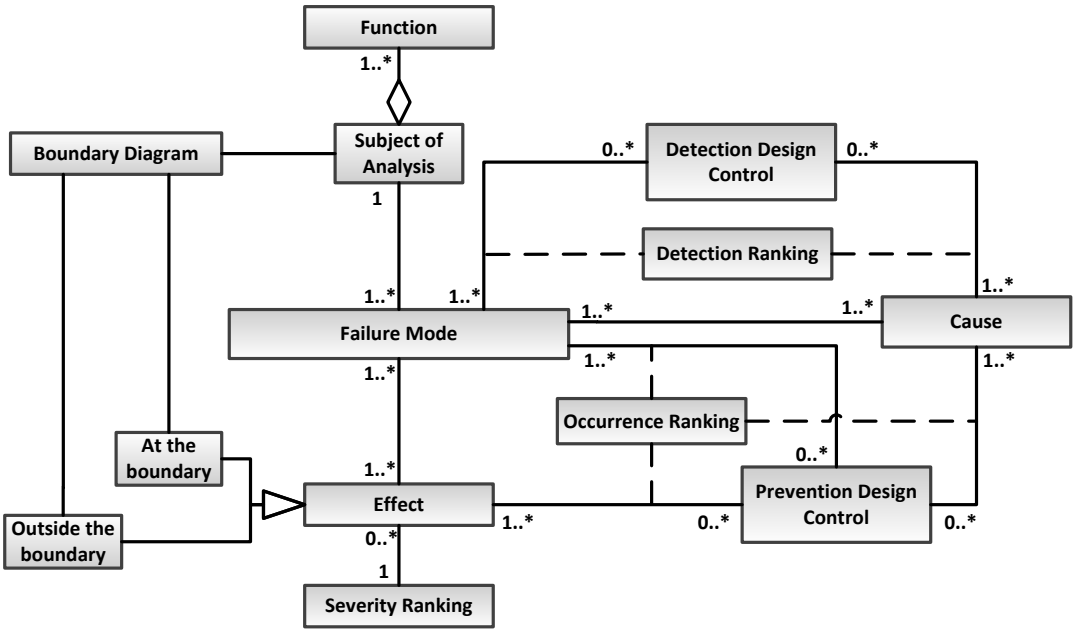

Figure 79: Ontology of FMEA Terms

A.4 Subject of analysis

This has to be defined. In J1739 this is referred to as the *item* while in the VDA document it is referred to as the *inspected product*. The content of the definition will depend on the level of abstraction at which the analysis is being performed and on the scope of analysis. The definition has to support the fact that a function will be analysed in terms of what *failure modes* it has and what the *cause* and *effect* of each *failure mode* is; this requires that the definition includes a decomposed structure that can be interpreted in terms of cause and effect. The functions may be defined quantitatively of qualitatively.

If the subject of analysis is the design of a physical object, then there will be a representation of a physical structure with each element of the structure having one or more functions. This is the approach taken explicitly in the VDA document. If the subject of analysis is a logical design, then it will only be a functional decomposition.

The scope of the analysis has to define where the consideration of *effects* in the cause-effect chain ends; this is usually represented by a boundary diagram. This shows functions at the boundary, which are within the scope of the analysis, and the interfaces to the environment, including the user, or other components or systems outside of the boundary. The scope also has to define where the consideration of *causes* in the cause-effect chain ends.

A.5 Failure Mode

Each function of the subject of analysis has one or more *failure modes;* these are identified by considering how a function may fail. J1739 states that as a minimum the analysis should consider *loss of function*, *partial function*, *intermittent function*, *degradation function* and *unintended function*. The VDA document gives examples as *non-conformities from specified target states*, *limited function*, *unintentional function* and *exceeding a function*. While IEC 60218 gives examples as *failure during operation*, *failure to operate at a prescribed time*, *failure to cease operation at a prescribed time* and *premature operation*.

A.6 Effect

The *effect* of a failure at the boundary of the subject of analysis is determined by an inductive analysis of the decomposed structure. The accuracy of this analysis is dependent on the detail and correctness of the defined decomposed structure. J1739 and IEC 60812 also recommend that the *effect* on the final product and/or the end customer be considered. If this involves understanding *effects* on components or systems outside the boundary diagram, then the necessary understanding is not included in the definition of the subject of analysis and has to be sought by consulting the relevant FMEAs or knowledgeable staff.

A.7 Severity Ranking

The severity of the *effect* is assessed qualitatively using an ordinal scale of 1 to 10. The *effect* is assessed for its impact on the environment or user. This may be because the *effect* has been traced through the decomposed structure to something that is outside the boundary or it may be an *effect* within the boundary which is directly perceived by the user, e.g. noise.

With the exception of severity rankings 9 and 10, the scale is not an absolute scale, but is calibrated relative to the subject of analysis. A *severity ranking* value of 10 is assigned if the *effect* impedes the safety operation of the vehicle. The value may be reduced to 9 if the driver is warned of the *effect* or failure and it is deemed that they have time to act to prevent harm from occurring. Table 35 shows the guidance for *severity rankings* given by J17399 and the VDA document.

A.8 Cause

The *cause* of a failure is determined by a deductive analysis of the decomposed structure. The difference between random and systematic *causes* of a failure is not explicitly mentioned. Again, the accuracy of this analysis is dependent on the detail and correctness of the defined decomposed structure. If traced to a physical component, then the *cause* will be expressed in terms of physical properties such as dimensions and tolerances, surface finish or material wear. The *cause* may be an input from outside the boundary. J1739 gives examples of typical *causes* as:

- Incorrect design for functional performance
- System interactions
- Changes over time
- Unanticipated external environment conditions
- Unanticipated customer use cycles
- Piece to piece variation
- Incorrect design for manufacturing

Failure *causes* may also be determined from analysis of field failures or failures in test units. When the design is new and without precedent, failure causes the analysis to rely on the opinion of experts.

	J1739:2009	**VDA:2006**
10	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.	Extremely severe failure that affects the safety and/or violates the compliance to legal regulations. Existence-endangering risk to the company
9	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.	
8	Loss of primary function (vehicle inoperable, does not affect safe vehicle operation)	Operability of the vehicle heavily limited and/or loss of functions that are necessary for normal driving. Immediate stay in the garage is imperatively
7	Degradation of primary function (vehicle operable, but at reduced level of performance)	
6	Loss of secondary function (vehicle operable, but comfort / convenience functions inoperable)	Operability of the vehicle limited, immediate stay in the garage is not necessary. Loss of important service and comfort systems.
5	Degradation of secondary function (vehicle operable, but comfort / convenience functions at reduced level of performance)	
4	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by most customers (> 75%)	
3	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by many customers (50%)	Low function impairment of the vehicle, limitation of function of important service and comfort systems
2	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by discriminating customers (< 25%)	
1	No discernible effect.	Very low function impairment, only identifiable by qualified personnel

Table 35: Guidance for FMEA Severity Rankings

A.9 Occurrence Ranking

The occurrence of the *cause*, *failure mode* or *effect* can be assessed qualitatively or quantitatively. The norm in the automotive domain is for it to be assessed qualitatively using an ordinal scale of 1 to 10. The assessment takes into account the *prevention design controls* that have been specified.

SAE 1739 describes a *prevention design control*, referred to as a *preventative action* in the VDA document, as a means to prevent a *cause*, *failure mode* or *effect* and gives examples as:

- Published design standard for thread class
- Heat treat specification on drawing
- Redundant design includes sensor shield
- Corporate best practice standard design
- System detection and driver notification for service
- System detection and operational status displayed to driver

SAE J1739 also recognises that *prevention design controls* can include means to detect and manage *causes* or *failure modes* during normal operation.

It is common practice to reassess the *occurrence ranking* after new *prevention design controls* have been specified. The occurrence scale is not an absolute scale but is calibrated relative to the subject of analysis. Table 2 shows the guidance for *occurrence rankings* given by J17399 and the VDA document.

	J1739:2009	**VDA:2006**
10	New technology/new design with no history.	New development of systems/components without operating experience and/or under unexplained operating conditions. Known system with problems.
9	Failure is inevitable with new design, new application, or change in duty cycle/operating conditions.	
8	Failure is likely with new design, new application, or change in duty cycle/operating conditions.	New development of systems/components using new technologies and/or use of previously problematic technologies. Known system with problems.
7	Failure is uncertain with new design, new application, or change in duty cycle/operating conditions	
6	Frequent failures associated with similar designs or in design simulation and testing.	New development of systems/components with operating experience and/or detail changes to previous development under comparable operating conditions. Mature systems/components with long, failure-free series production experience under altered operating conditions.
5	Occasional failures associated with similar designs or in design simulation and testing.	
4	Isolated failures associated with similar design or in design simulation and testing.	
3	Only isolated failures associated with almost identical design or in design simulation and testing.	New development of systems/components with positively completed proof procedure. Detail changes to mature systems/components with long failure free series production experience under comparable operating conditions.
2	No observed failures associated with almost identical design or in design simulation and testing	
1	Failure is eliminated through preventative control	New development and/or mature systems/components with operating experience under comparable (differentiation to 3-2 necessary!) operating conditions with positively completed proof procedure. Mature systems/components with long, failure-free series production experience under comparable operating conditions.

Table 36: FMEA Guidance for Occurrence Rankings

A.10 Detection Ranking

As well as *prevention design controls*, *detection design controls* can also be specified. J1739 describes a *detection design controls*, referred to as *detective action* in the VDA document, as a means to detect a *cause* and/or *failure mode*, either by analytical or physical methods, before the item is released to production, and gives examples as:

- Finite Element Analysis (FEA)
- CAE analytics
- Tolerance stack analysis
- Validation testing (fatigue, water intrusion, vibration, ride and handling, etc.)

It is common practice to reassess the *detection ranking* after new *detection design controls* have been specified.

The effectiveness of the *detection design controls* specified is assessed qualitatively using an ordinal scale of 1 to 10. The detection scale is not an absolute scale but is calibrated relative to the subject of analysis. Table 37 shows the guidance for *detection rankings* given by J17399 and the VDA document.

	J1739:2009	**VDA:2006**
10	No current design control; Cannot detect or is not analyzed	Failure with a very low detection potential, since a proof procedure is not known and/or has not been established
9	Design analysis/detection controls have a weak detection capability; Virtual Analysis (e.g. CAE, FEA, etc.) is **not correlated** to expected actual operating conditions.	
8	Product verification/validation after design freeze and prior to launch with **pass/fail** testing (Sub-system or system testing with acceptance criteria e.g. Ride & handling, shipping evaluation, etc.)	Failure with a low detection potential, since the proof procedure is uncertain and/or there is no experience with the established proof procedure
7	Product verification/validation after design freeze and prior to launch with **test to failure** testing (Sub-system or system testing until failure occurs, testing of system interactions, etc.)	
6	Product verification/validation after design freeze and prior to launch with **degradation** testing (Sub-system or system testing after durability test e.g. Function check)	Failure with a moderate detection potential. Mature proof procedure from comparable products under new usage/boundary conditions
5	Product validation (reliability testing, development or validation tests) prior to design freeze using **pass/fail** testing (e.g. acceptance criteria for performance, function checks, etc.)	
4	Product validation (reliability testing, development or validation tests) prior to design freeze using **test to failure** (e.g. until leaks, yields, cracks, etc.)	
3	Product validation (reliability testing, development or validation tests) prior to design freeze using **degradation** testing (e.g. data trends, before/after values, etc.)	Failure with a high detection potential due to mature proof procedure. The effectiveness of the detection action has been demonstrated for this product.
2	Design analysis/detection controls have a strong detection capability. Virtual Analysis (e.g. CAE, FEA, etc.) is **highly correlated** with actual and/or expected operating conditions prior to design freeze.	
1	Failure cause or failure mode cannot occur because it is fully prevented through design solutions (e.g. Proven design standard/best practice or common material, etc.)	Failure with a very high detection potential due to mature proof procedure of previous generation. The effectiveness of the detection action has been demonstrated for this product.

Table 37: FMEA Guidance for Detection Rankings

A.11 Criticality Analysis

The significance of the identified *failure modes*, *effects* and *causes* can be assessed based on the rankings for severity, occurrence and detection have been assigned. Different approaches can be taken. One approach is to just assess significance based on the *severity ranking*, with a ranking of 9 or 10 being designated as critical. Another approach is to assess the severity and occurrence rankings together and designating a defined combination of rankings as being significant. Such classifications can be used to assign *special characteristics* to particular *failure modes* or *causes* to signify that they can have an impact on factors such as safety or compliance to regulations. *Special characteristics* are defined by each organisation. Alternatively, or as well as, the three values may be multiplied together to produce a Risk Priority Number (RPN). This last approach has been criticised by several authors, [173], [174]; the latter on the basis that the scales are ordinal and that an interval scale is required in order for the multiplication operation to be valid.

Appendix B ISO 26262 Exposition

B.1 Introduction

ISO 26262, Road vehicles - Functional safety, [13], is an adaptation of the generic functional safety standard IEC 61508, [12], to meet the specific needs of electrical and/or electronic (E/E) systems within road vehicles. An *E/E system* is defined as a system that consists of electrical and/or electronic elements, including programmable electronic elements, while an element is defined as a system or part of a system including components, hardware, software, hardware parts and software units. A system is defined as a set of elements that relates at least a sensor, a controller and an actuator with one another.

Its requirements cover all activities during the safety lifecycle, Figure 80, of safety-related systems comprised of electrical, electronic and software components. The purpose of the standard is to provide guidelines for how to avoid *unreasonable residual risk* associated with an *E/E system*. *Unreasonable risk* is defined as "*risk judged to be unacceptable in a certain context according to valid societal moral concepts*".

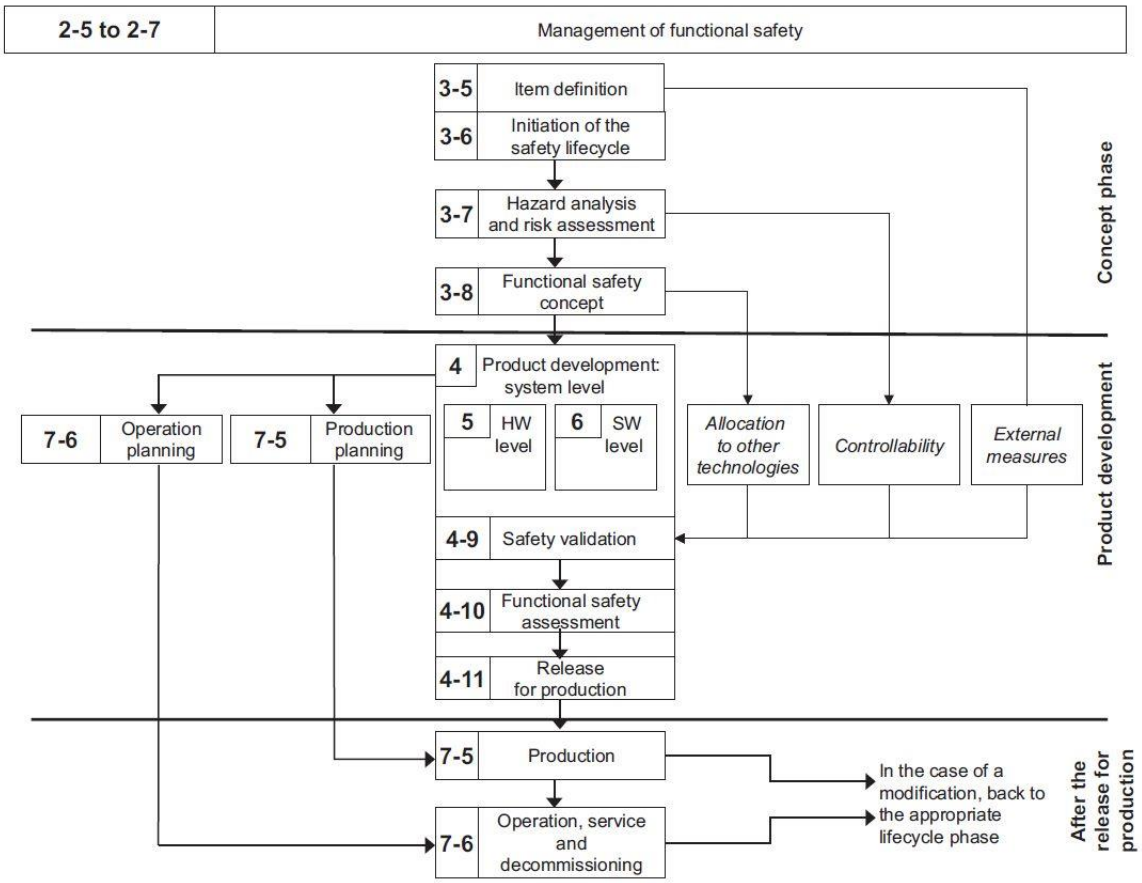

Figure 80: ISO 26262 Safety Lifecycle

The scope of the risk addressed is limited to failure, or unintended behaviour, of an *item* with respect to its design intent. The term *item* is defined as a system, or an array of systems, to implement a

function at the vehicle level, to which ISO 26262 is applied. The standard does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour *of E/E safety-related systems*. Also, the standard does not address the nominal performance of *E/E systems*.

Like IEC 61508, ISO 26262 is based around a safety life cycle that starts with identifying *hazards* and covers development, manufacture, service and disposal. The standard is published in ten parts:

- Part 1: Vocabulary
- Part 2: Management of functional safety
- Part 3: Concept phase
- Part 4: Product development at the system level
- Part 5: Product development at the hardware level
- Part 6: Product development at the software level
- Part 7: Production and operation
- Part 8: Supporting processes
- Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
- Part 10: Guideline on ISO 26262

The first edition was published in 2011. While not a legal requirement, i.e. it is not part of any regulations that must be met to sell the vehicle, it is viewed by the industry as a statement of best practice which would form the basis of any defence in a product liability case. A second edition is due to be published in 2018 which will have an additional two parts:

- Part 11: Guideline on application of ISO 26262 to semiconductors
- Part 12: Adaptation for motorcycles

The standard can be summarised by the following objectives:

- To have an appropriate organisation
- To perform appropriate planning and project management
- To derive and specify appropriate functional safety requirements at the functional, technical, hardware and software levels such that *unreasonable risk* is avoided
- To ensure that functional safety requirements are not violated by faults and failures; achieved by analysing the design to identify faults and failures and then mitigating them by defining additional functional safety requirements
- To produce a design that fulfils the functional safety requirements
- To verify that the design meets the functional safety requirements
- To validate that *unreasonable risk* has been avoided
- To achieve all of the above by using a systematic rigorous process that conforms with the current understanding of best practice

In this exposition we consider risk assessment, safety requirements, integrity and functional safety assessment. Organisation, project management, production and operation are not described.

B.2 Risk Assessment

The risk assessment is based on the *item definition*; in the body of the standard this term is used to refer to the target of the development. An *item* is defined as a system, or an array of systems, to implement a function at the vehicle level, to which ISO 26262 is applied. The standard requires that the *item* be documented in a work-product called the *Item Definition*. The purpose of this work-product is to define and describe the *item*, its dependencies on, and interaction with, the environment and other *items,* in order to support activities in subsequent phases.

Consistent with its scope, ISO 26262 requires that the risk of a malfunctioning *E/E system* be determined by considering the effects of the malfunction; such a malfunction is termed a *hazard* if it has the potential to cause harm. Malfunctions are identified based on the description given in the *Item Definition*; this includes the capabilities of the actuators, as this information is necessary assessing the values of *severity* and *controllability*.

The risk assessment considers the probability that an accident will be the outcome of a *hazard* and also the most likely *severity* of the accident. The risk assessment is described in Chapter 6 using the general conditional probability risk model; here we replace *faulty-machine-behaviour* with *hazard*:

$$P_{harm} = P_{fault} * P[hazard \mid fault] * P[harm \mid hazard]$$

The ISO 26262 requirement for risk assessment is to evaluate $P[harm \mid hazard]$ assuming that $P_{fault} * P[hazard \mid fault]$ has a value of 1. $P[harm \mid hazard]$ is the probability that an accident will be the outcome of a *hazard* because the *harm* is a consequence of the accident. A *hazard* is always defined at a vehicle level in terms of what the driver would experience, or a third party observe, in the event of a malfunction of the *item*. *Hazards* may be determined by considering the consequences of the *item's* functions, as defined in the *Item Definition*, not being performed as intended and also by considering what an actuator has the capability to produce, e.g. maximum force exerted.

The harm that may result from a *hazard* depends on the *operational situation* that the vehicle is in at the time, as this determines the accident sequence The assessment includes both those situations when the vehicle is used correctly and those when it is used is incorrectly, in a foreseeable way. The combination of a *hazard* and an *operational situation* is referred to as a *hazardous event* and it is for each of the latter that $P[harm \mid hazard]$ is assessed . The assessment estimates the probability that the vehicle enters the *operational situation*. This is expressed as value of *exposure,* and the probability that human actions can avoid the harm associated with the consequence; this is expressed as a value of *controllability*.

The values, and their descriptions, used to express e*xposure* are:

- E0 - incredible
- E1 - very low probability
- E2 - low probability
- E3 - medium probability
- E4 - high probability

The values are not given any further definition, but informative examples are provided and the standard expects there to be an order of magnitude difference in probability between adjacent values. *Exposure* can be estimated by considering the duration of time spent in the *operational situation* or the frequency with which the *operational situation* is encountered. If the estimated value is *E0*, then the risk assessment is not completed.

The values, and their descriptions, used to express *controllability* are:

- C0 - controllable in general
- C1 - simply controllable
- C2 - normally controllable
- C3 - difficult to control or uncontrollable

The values are not given any further definition, but informative examples are provided and the standard expects there to be an order of magnitude difference in probability between adjacent values. The estimation of the value takes into account the potential actions of all people who could influence the outcome, including third parties who may not be directly involved. If the estimated value is *C0*, then the risk assessment is not completed.

The probability that an accident will result, given the presence of a *hazard*, can be expressed as the combination of four values of *exposure* and three values of *controllability*, i.e. twelve in total. The estimate of the severity of the *harm* caused by the accident is expressed as a value of *severity*. The values, and their descriptions, used to express *severity* are:

- S0 - no injuries
- S1 - light and moderate injuries
- S2 - severe and life-threatening injuries (survival probable)
- S3 - life-threatening injuries (survival uncertain), fatal injuries

The values are not given any further definition, but informative examples are provided. The estimation considers all those who could potentially be injured including the vehicle driver and passengers, cyclists, pedestrians and the occupants of other vehicles. The estimation may be based on a combination of injuries. If the estimated value is *S0*, then the risk assessment is not completed.

The outcome of the risk assessment is denoted by the terms *QM*, *ASILA*, *ASILB*, *ASILC* and *ASILD*[5] which are labels for sets of combinations of *exposure*, *controllability* and *severity* values, Table 38.

Result of Risk Assessment	**Combination of exposure, controllability and severity**
QM	((E1, C1), S1), ((E1, C2), S1), ((E1, C3), S1), ((E2, C1), S1), ((E2, C2), S1), ((E2, C3), S1), ((E3, C1), S1), ((E3, C2), S1), ((E4, C1), S1), ((E1, C1), S2), ((E1, C2), S2), ((E1, C3), S2), ((E2, C1), S2), ((E2, C2), S2), ((E3, C1), S2), ((E1, C1), S3), ((E1, C2), S3), ((E2, C1), S3)
ASILA	((E3, C3), S1), ((E4, C2), S1), ((E3, C2), S2), ((E2, C3), S2), ((E3, C2), S2), ((E4, C1), S3), ((E2, C2), S3), ((E3, C1), S3)
ASILB	((E4, C3), S1), ((E3, C3), S2), ((E4, C2), S2), ((E2, C3), S3), ((E3, C2), S3), ((E4, C1), S3)
ASILC	((E4, C3), S2), ((E3, C3), S3), ((E4, C2), S3)
ASILD	((E4, C3), S3)

Table 38: ISO 26262 Risk Assessment Outcomes

The risk analysis is based on the definition of the *item* without taking account of the specification or implementation of any safety requirements. In this thesis, this is referred as an assessment of the unmitigated risk. Risk mitigation is associated with deriving safety requirements as described in section B.3. The labels that are used to denote the unmitigated risk are also used to indicate the integrity with which safety requirements are to be implemented as described in section B.4.

B.3 Safety Requirements

B.3.1 Safety Goals

The derivation of the safety requirements begins with the specification of *safety goals*. A *safety goal* is a top-level safety requirement, phrased in terms of a functional objective, related to the prevention or mitigation of hazardous events, such that *unreasonable risk* is avoided. For each *hazardous event* one or more *safety goals* are defined. A *safety goal* can be related to more than one *hazardous event*.

The standard recognises the concept of *residual risk* which it defines as the risk remaining after the deployment of *safety measures*[6] and *safety mechanisms*[7]. The implication is that for the standard to be met, the *residual risk* should be less than or equal to *unreasonable risk*. The standard does not

[5] QM stands for Quality Management, ASIL stands for Automotive Integrity Level
[6] A safety measure is an activity, or technical solution, to avoid, or control, systematic failures and to detect, or control, random hardware failures or mitigate their harmful effects. They include safety mechanisms.
[7] A safety mechanism is technical solution to detect faults or control failures in order to achieve or maintain a safe state as defined in the functional safety concept.

give any guidance on how to decide if a *safety goal* will result in a *residual risk* less than or equal to *unreasonable risk*.

MISRA, [200], advocates the following interpretation. Having defined one or more *safety goals* for a *hazardous event* it is necessary to determine what the *residual risk* would be if the goals are met. There is only one risk assessment scheme given in the standard, as described above, so to determine the *residual risk* it is necessary to use this scheme to determine the risk of the *hazardous event*, assuming that the *safety goal(s)* has been met. As the determination of risk is based around the estimation of *severity*, *exposure* and *controllability*, the meeting of a *safety goal* would reduce one or more of these three factors. As the lowest value of risk that be denoted is *QM*, MISRA takes the view that an adequate *safety goal* is one which, if met, would result in a *residual risk* of *QM*.

If the *safety goal* is formulated in the style of "*the hazard shall not occur*", as is the case with the 4CAS example, then it is not useful to assess the *residual risk* assuming the goal is met. In these cases, the residual risk has to be assessed based on the functional safety concept being achieved.

Safety goals are validated for the *item* integrated in a representative vehicle to demonstrate that they are fully achieved at the vehicle level.

B.3.2 Functional Safety Concept

A *functional safety concept* (FSC) is defined as the specification of the *functional safety requirements*, with associated information, their allocation to architectural elements, and their interaction necessary to achieve the *safety goals*. The FSC can take account of *external measures* which are defined as a measure that is separate and distinct from the *item* which reduces or mitigates the risks. The FSC can also take account of *other technologies*, which are defined as technologies different from E/E technologies within the scope of ISO 26262. The FSC is defined in functional terms only and is implementation-free.

The *functional safety concept* is verified to show that it is consistent with, and compliant with, the safety goal, and that it has the ability to mitigate or avoid the *hazardous events*.

B.3.3 Technical Safety Concept

A *technical safety concept* (TSC) is defined as a specification of the *technical safety requirements* and their allocation to *system elements* for implementation by the system design. The *technical safety requirements* are derived from the implementation-free *functional safety requirements* and allocated to the actual implementation represented by the system design. The system design specifies the requirements for the hardware and software that ultimately constitute the *E/E system*[8].

[8] The four levels of design, FSC, TSC, hardware and software are used by the standard for explanatory purposes, in practice, depending on the definition of the *E/E system*, all of these four levels can have subdivisions and it is up to the user of the standard to apply the concepts to their particular development.

The standard uses a model for both hardware and software whereby requirements are allocated to an architecture which consists of components, which may be hierarchical assembles of other components, before terminating in *hardware parts* and *software units*. The *software units* are compiled into object-code and contained within a *hardware part*. The standard also requires that a *hardware-software interface* specification be created to specify the hardware and software interaction, e.g. hardware devices that are controlled by software and hardware resources that support the execution of software.

The system design is analysed to identify the causes and effects of systematic faults, and actions are taken to eliminate the causes or mitigate the effects. The system design is verified for compliance and completeness with regard to the TSC. Also, the following integration testing is also performed:

- hardware-software integration testing
- system integration and testing
- vehicle integration and testing

B.3.4 Hardware Safety Requirements

The *hardware safety requirements* are derived from the *technical safety requirements*, and the *hardware-software interface* specification, and allocated to elements of the hardware design.

The hardware design is evaluated for robustness against random hardware faults that could result in the violation of a *safety goal*. Three metrics are used:

- single-point fault metric
- latent-fault metric
- evaluation of safety goal violations due to random hardware failures

Single-point fault metric and latent-fault metric

The purpose of these metrics is to guide the hardware design and show that it complies with the *safety goals*. The target values may be derived from the hardware architectural metrics calculation applied on similar well-trusted design principles or derived from some indicative values given in the standard.

The assessment of the hardware design against these targets may be based on meeting the target value for the whole hardware design, or else justifying that meeting a target at the hardware element level is sufficient to comply meeting the target value for whole hardware design. Additionally, the assessment of the latent-fault metric target value may be based on meeting the target values for the diagnostic coverage for each hardware element with faults that can lead to the unavailability of a safety mechanism.

Evaluation of safety goal violations due to random hardware failures

The purpose of this evaluation is to "*make available criteria that can be used in a rationale that the residual risk of a safety goal violation, due to random hardware failures of the item, is sufficiently low.*" This may be achieved by either meeting the *Probabilistic Metric for Random Hardware Failures* (PMHF) or by performing an evaluation of each cause of *safety goal* violation.

A target value for the PMHF may be derived from field data from similar well-trusted design principles, derived from quantitative analysis techniques applied to similar well-trusted design principles, or derived from some indicative values given in the standard. The target values do not have any absolute significance and are only useful to compare a new design with existing ones. The assessment of the hardware design against these targets involves calculating the total failure rate based on the failure rates of all components.

An alternative method for evaluating *safety goal* violations due to random hardware failures is also given, based on improving the diagnostics coverage.

The hardware design is verified for compliance and completeness with respect to the *hardware safety requirements*.

B.3.5 Software Safety Requirements

The *software safety requirements* are derived from the *technical safety requirements*, and the *hardware-software interface* specification, and allocated to elements of the software architecture.

The software architecture is analysed to identify safety-related parts of the software and support the specification of *safety mechanisms* associated with random hardware failures and systematic software faults. If the implementation of *software safety requirements* relies on freedom from interference, or sufficient independence between software components, then an analysis is performed to establish that the requirements for freedom from interference and independence have been met

The software architecture is verified for compliance with the *software safety requirements*, compatibility with the target hardware and adherence to design guidelines.

B.4 Integrity

As mentioned above, the standard uses the terms, *safety measures* and *safety mechanisms*. It does not prescribe the *safety mechanisms* as these are particular to each *E/E system* developed. The standard does prescribe the use of particular *safety measures*, excluding the *safety mechanisms*, as these are common to all developments. The prescription is achieved by reusing the labels that denote the unmitigated risk to indicate the integrity with which safety requirements are to be implemented. To this end, all safety requirements, i.e. *safety goals*, *functional safety requirements*, *technical*

safety requirements, *hardware safety requirements* and *software safety requirements*, are assigned a label which can take values of *ASILA*, *ASILB*, *ASILC* or *ASILD*. The label takes its value from the one that denotes the unmitigated risk of the *hazardous event* from which the safety requirements are derived. The values may be reduced using a process referred to as *requirements decomposition with respect to ASIL tailoring* (aka ASIL decomposition) which requires that the intent of a safety requirement be achieved by two independent means.

In the parts 2, 4, 5, 6 and 8 of ISO 26262, the clauses, or sub-clauses, of the standard are stated as being applicable to safety requirements, or activities related to them, depending on their associated integrity value. The standard indicates the applicability as *ASILA*, *ASIL(A)*, *ASILB*, *ASIL(B)*, *ASILC*, or *ASILD*. These occur in the following combinations:

- *ASILA*, *ASILB*, *ASILC*, *ASILD* (often indicated by the word "all")
- *ASILB*, *ASILC*, *ASILD*
- *ASILC*, *ASILD*
- *ASILB*
- *ASILC*
- *ASILD*
- *ASIL(A)*, *ASILB*, *ASILC*, *ASILD*
- *ASIL(A)*, *ASIL(B)*, *ASILC*, *ASILD*
- *ASIL(A)*, *ASIL(B)*, *ASIL(C)*, *ASILD*
- *ASIL(B)*, *ASILC*, *ASILD*

An *ASIL* value given in parentheses indicates that the corresponding clause, or sub-clause, is only a recommendation. The clauses, or sub-clauses, whose applicability depends on the ASIL value, are related to analysis methods, design properties, verification methods, hardware metrics targets, software modelling/coding guidelines, notations for software design and software design principles. The safety requirements are deemed to be implemented with the required integrity if the corresponding clauses, or sub-clauses are complied with.

B.5 Functional Safety Assessment

The standard requires a number of confirmation measures to be performed. The independence of the staff performing these measures is determined by the ASIL value associated with the *item*. These measures are:

- Confirmation review of designated work-products to evaluate their compliance corresponding clauses, or sub-clauses of ISO 26262
- Functional safety audit of the activities performed against those specified in the safety plan

- Functional safety assessment of the *item* described in the *item definition* by examination of the work-products required by the safety plan, the implementation of the required processes and a review of the implemented safety measures

The standard also calls for a safety case to be developed which it defines as argument that the safety requirements for an *item* are complete and satisfied by evidence compiled from work-products of the safety activities performed during development.

Appendix C Mechatronic Safety Argument

In Chapter 4 we showed how the 4CAS design material related to the generic blocks of the ontology as an example of how a *mechatronic system* could be divided into a set of *Partes*. In this Appendix we show how the material can support the 4CAS safety argument. We start with a single hazardous event identified by the 4CAS analysis and show how the argument can be constructed from the mechatronic pattern given in Chapter 4. In constructing the argument, we bring in other data from the 4CAS development, or discuss what the data could have been. The scope of this example argument is *Pars 1*, *Pars 2* and *Pars 3*. It is restricted to only three *Partes* for practical reasons, as the volume of material referenced by the argument increases significantly after *Pars 3*.

In *Pars 1*, we are arguing over a specific *hazardous event* and then a *safety goal* which addresses several *hazardous events*. In *Pars 2*, we are arguing over a *mechatronic functional safety concept* that addresses the *safety goal* from *Pars 1*. In the *Pars 3*, we are arguing over a *mechatronic technical safety concept* which addresses all *mechatronic functional safety concepts*, so it is no longer specific to the starting *hazardous event*.

The skeleton of the whole argument for *Pars 1*, *Pars 2* and *Pars 3* is shown in Figure 81, using the GSN notation. The argument structure closely follows the mechatronic one given in Chapter 4. Here, we have not included the cascading of material from one *Partes* to another and instead have shown the connection by using a common *context*. The identifiers in the symbols are explained in the text that follows for each *Pars*. The naming convention is that the same identifiers are used as for the mechatronic argument pattern given in Chapter 4, but prefixed with the letter "E".

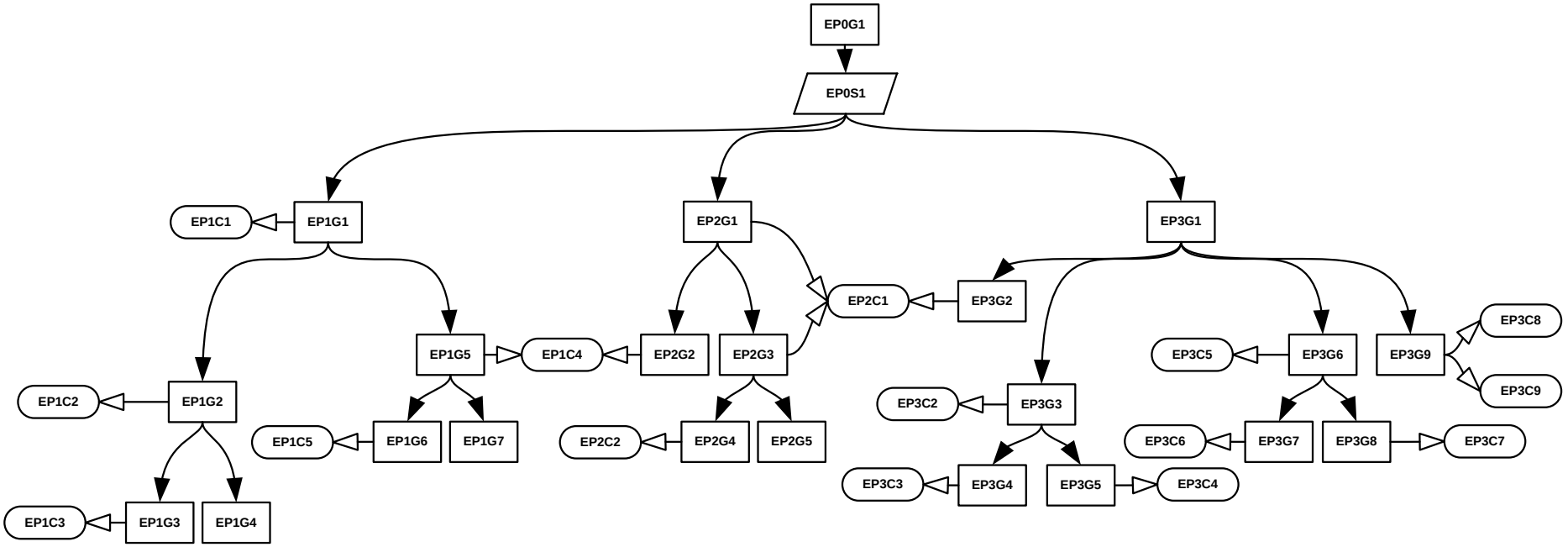

Figure 81: Whole 4CAS Safety Argument

C.1 Pars 1: Mechatronic Item Definition and Hazard & Risk Assessment

The *Pars 1* argument structure is shown in Figure 82, it is based on Figure 48. The symbols are defined in Table 39 which shows the mechatronic pattern text and the 4CAS example.

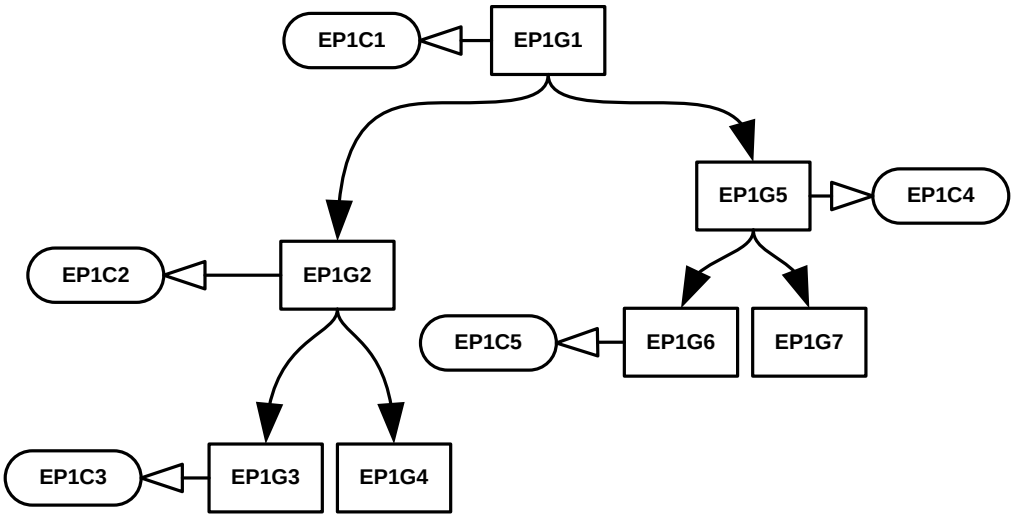

Figure 82: Pars 1 Argument Structure

Identifier	Symbol	Mechatronic Pattern Text	4CAS Example Text
EP1G1	Claim	The Mechatronic HARA Documentation meets its ISO 26262 requirements	4CAS HARA documentation meets ISO 26262 requirements
EP1C1	Context	Reference to initial system material used to create the Mechatronic Item Definition	Section 4.1 4CAS description (Design artefact)
EP1G2	Claim	All Hazardous Events meet their ISO 26262 requirements	All 4CAS Hazardous Events meet their ISO 26262 requirements
EP1C2	Context	P2B2: Hazardous Events	Different to Expected Oversteer in bend (Design artefact)
EP1G3	Claim	All properties required of the Hazardous Events have been achieved	All properties of the 4CAS Hazardous Event Properties have been achieved
EP1C3	Context	Hazardous Event Properties	ASIL classification
EP1G4	Claim	All Hazardous Events have been defined in compliance with ISO 26262	All 4CAS Hazardous Events have been defined in compliance with ISO 26262
EP1G5	Claim	All Mechatronic Safety Goals meet their ISO 26262 requirements	All 4CAS Safety Goals meet their ISO 26262 requirements
EP1C4	Context	Mechatronic Safety Goals	4CAS SG2: The vehicle users, and other road users, shall not be exposed to unacceptable risk due to gross height or pressure errors at the 4 corners, ASIL B. (Design artefact)
EP1G6	Claim	All properties required of the Mechatronic Safety Goal have been achieved.	All properties required of the 4CAS Safety Goal have been achieved.
EP1C5	Context	Mechatronic Safety Goal Properties	If met, the Safety Goal must avoid unreasonable risk
EP1G7	Claim	All Mechatronic Safety Goals have been defined in compliance with ISO 26262	All 4CAS Safety Goals have been defined in compliance with ISO 26262

Table 39: Pars 1 Symbols

C.1.1 EP1G1

Claim *EP1G1*: *4CAS HARA documentation meets ISO 26262 requirements* is the start of the whole argument structure. ISO 26262 states what the *item definition* should contain, but does not require it to have verification reviews, so the question of whether it is complete and correct is not addressed. The MISRA framework seeks to address this with an argument that links the completeness of the *hazardous events* with the completeness of the *item definition*. These issues were not formally addressed in the 4CAS development; the completeness and correctness were assured by virtue of a small team of experts working closely together.

For the purposes of the example, the initial material, *EP1C1*, is that given in Chapter 4, section 4.1 4CAS description. In our model, this *context* represents a design artefact.

C.1.2 EP1G2

For claim *EP1G2: All 4CAS Hazardous Events meet their ISO 26262 requirements* we are using just the single *hazardous event* given in *context EP1C2* as *Different to Expected Oversteer in bend*[9]. This is a combination of *hazard - Different to Expected Oversteer*, and the *operational situation - negotiating a bend of moderate curvature at a speed greater than 50 mph*. In our model, this *context* represents a design artefact.

The properties of a *hazardous event*, *context EP1C3*, as adapted from ISO 26262, is that it has the correct ASIL value classification. In this example the claim *EPG3* is met by the *hazardous event - Different to Expected Oversteer in bend* being classified as *ASILB.*

The claim *EP1G4: All Hazardous Events have been defined in compliance with ISO 26262* could be developed using claims related to process, review and audit. The MISRA Safety Case Guidelines makes many suggestions for *means* and *organisational environment* claims along these lines.

C.1.3 EP1G5

For claim *EP1G5: All 4CAS Safety Goals meet their ISO 26262 requirements* there is a single *safety goal, EP1C4: SG2: The vehicle users, and other road users, shall not be exposed to unacceptable risk due to gross height or pressure errors at the 4 corners, (ASIL B).* This *safety goal* addresses a group of *hazardous events* including *Different to Expected Oversteer in bend*. In our model this *context* represents a design artefact.

The properties of a *mechatronic safety goal*, *context EP1C5*, as adapted from ISO 26262, is that meeting the *mechatronic safety goal* avoids unreasonable risk. In this example, the claim *EP1G6* is met by the following rationale:

[9] This 4CAS hazardous event is only indicative

- Oversteer is caused by height or pressure errors at the four corners
    - There is analysis which provides evidence to support this statement
- The *mechatronic safety goal* is defined as requiring unreasonable risk to be avoided

The claim *EP1G7: All Mechatronic Safety Goals have been defined in compliance with ISO 26262* could be developed using claims related to process, review and audit. The MISRA Safety Case Guidelines makes many suggestions for *means* and *organisational environment* claims along these lines. Note that the safety goal has inherited the ASIL value in accordance with ISO 26262.

C.2 Pars 2: Mechatronic Functional Safety Concept

The *Pars 2* argument structure is shown in Figure 83, it is based on Figure 57. The symbols are defined in Table 40, which shows the mechatronic pattern text and the 4CAS example.

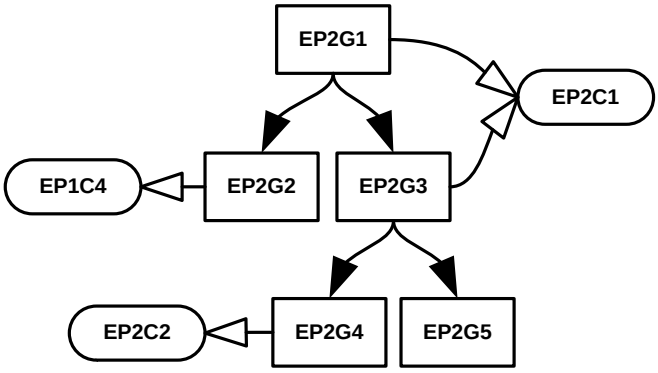

Figure 83: Pars 2 Argument Structure

Identifier	Symbol	Mechatronic Pattern Text	4CAS Example Text
EP2G1	Claim	The Mechatronic Functional Safety Concept meets its ISO 26262 requirements	4CAS Mechatronic Functional Safety Concept meets its ISO 26262 requirements (Design artefact)
EP2C1	Context	Mechatronic Functional Safety Concept	4CAS Mechatronic Functional Safety Concept
EP2G2	Claim	The Documentation that the Mechatronic Functional Safety Concept is based on is complete and correct	4CAS Safety Goals are complete and correct
EP1C4	Context	Mechatronic Safety Goals	4CAS Safety Goals
EP2G3	Claim	Mechatronic Functional Safety Concept meets its ISO 26262 requirements	4CAS Mechatronic Functional Safety Concept meets its ISO 26262 requirements
EP2G4	Claim	All properties required of the Mechatronic Functional Safety Concept have been achieved.	All properties required of the 4CAS Mechatronic Functional Safety Concept have been achieved.
EP2C2	Context	Mechatronic Functional Safety Concept Properties	4CAS Mechatronic Functional Safety Concept Properties
EP2G5	Claim	Mechatronic Functional Safety Concept has been defined in compliance with ISO 26262	4CAS Mechatronic Functional Safety Concept has been defined in compliance with ISO 26262

Table 40: Pars 2 Symbols

C.2.1 EP2G2

The *mechatronic functional safety concept* is based on the *mechatronic safety goals* which were derived in *Pars 1*; their completeness and correctness was argued there, *EP1G6* and *EP1G7*. The claim *EP2G2: The Documentation that the Mechatronic Functional Safety Concept is based on is complete and correct* is effectively a repeat of this claim. If the *mechatronic functional safety concept* is created in the same work package, e.g. the same staff in the same organisation, then the claim would be based on the local change control and version management systems and the governance of these. If *mechatronic functional safety concept* was not created in this way, then the argument would be based on the information provided by the organisation responsible for deriving the *mechatronic safety goals*.

C.2.2 EP2G3

The claim *EP2G3: 4CAS Mechatronic Functional Safety Concept meets its ISO 26262 requirements* relates to the design artefact that defines the concept as referenced in *EP2C1*. In the 4CAS example this was contained the design artefact *4CAS Functional Safety Concept@1_7.pdf*. Its content included:

- Assumptions concerning the roll stability at different heights and the effects on roll stability of the brakes Dynamic Stability Control function
- Nominal behaviour safety requirements stating required behaviour during fault-free operation; these are also shown in the activity diagrams of Figure 58 and Figure 59
- Fault management safety requirements stating what system failures shall be detected and the 4CAS system response to those failures; these are also shown in the activity diagrams of Figure 60, Figure 61 and Figure 62.

The properties of a *mechatronic functional safety concept*, *context EP2C1*, as adapted from ISO 26262, is that it achieves all its associated *mechatronic safety goals*. However, given the formulation of the safety goal in this case, the property that must be established is that normally associated with the *mechatronic safety goal*, namely that a correctly implemented *mechatronic functional safety concept* avoids unreasonable risk. In our example a rationale, based on the stated assumption and safety requirements, is given in the design artefact *4CAS Functional Safety Concept@1_7.pdf*.

The claim *EP2G5: 4CAS Mechatronic Functional Safety Concept has been defined in compliance with ISO 26262* could be developed using claims related to process, review and audit. The MISRA Safety Case Guidelines makes many suggestions for means and organisational environment claims along these lines.

C.3 Pars 3: Mechatronic Technical Safety Concept

The *Pars 3* argument structure is shown in Figure 84, it is based on Figure 61. The symbols are defined in Table 41 which shows the mechatronic pattern text and the 4CAS example.

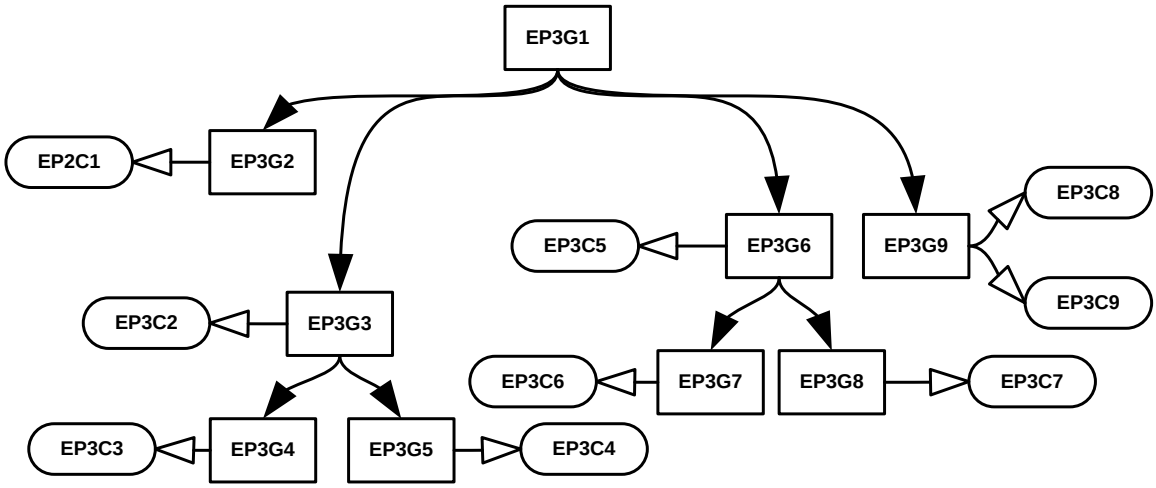

Figure 84: Pars 3 Argument Structure

C.3.1 EP3G2

The *mechatronic technical safety concept* is based on the *mechatronic functional safety concept* which was derived in *Pars 2*; its completeness and correctness was argued there, *EP2G4* and *EP2G5*. The claim *EP3G2: The Documentation that the Mechatronic Technical Safety Concept is based on is complete and correct* is effectively a repeat of this claim. If the *mechatronic technical safety concept* is created in the same work package, e.g. the same staff in the same organisation, then the claim would be based on the local change control and version management systems and the governance of these. If *mechatronic technical safety concept* was not created in this way, then the argument would be based on the information provided by the organisation responsible for deriving the *mechatronic functional safety concept*.

C.3.1 EP3G3

The claim *EP3G3: All 4CAS Mechatronic Technical Safety Requirements achieves all their required properties* relates to the design artefact that specifies the requirements as referenced in *EP3C2*. In the 4CAS example the *E/E system* requirements were recorded in a proprietary electronic database, eLog. Those related to the mechanical design were managed by the Chassis department and are not available. There was no requirement for a single *mechatronic technical safety requirements* document.

Identifier	Symbol	Mechatronic Pattern Text	4CAS Example Text
EP3G1	Claim	All Mechatronic Technical Safety Concept artefacts achieve their required properties	All 4CAS Mechatronic Technical Safety Concept artefacts achieve their required properties (Design artefact)
EP2C1	Context	Mechatronic Functional Safety Concept	4CAS Mechatronic Functional Safety Concept
EP3G2	Claim	The Documentation that the Mechatronic Technical Safety Concept is based on is complete and correct	4CAS Mechatronic Functional Safety Concept is complete and correct
EP3C2	Context	Mechatronic Technical Safety Requirements	4CAS Mechatronic Safety Technical Requirements
EP3G3	Claim	All Mechatronic Technical Safety Requirements achieves all their required properties	All 4CAS Mechatronic Technical Safety Requirements achieves all their required properties
EP3C3	Context	Mechatronic Technical Safety Requirement Properties	4CAS Mechatronic Technical Safety Requirement Properties
EP3G4	Claim	All properties required of the Mechatronic Technical Safety Requirements have been achieved.	All properties required of the 4CAS Mechatronic Technical Safety Requirements have been achieved.
EP3C4	Context	Mechatronic Technical Safety Requirement Process	4CAS Mechatronic Technical Safety Requirement Process
EP3G5	Claim	All Mechatronic Technical Safety Requirements have been defined in compliance with the process	All 4CAS Mechatronic Technical Safety Requirements have been defined in compliance with the process
EP3C5	Context	Mechatronic System Design	4CAS example diagrams from Chapter 4 Would be other documentation as well, not shown here
EP3G6	Claim	The Mechatronic System Design achieves all its required properties	The 4CAS Mechatronic System Design achieves all its required properties
EP3C6	Context	Mechatronic System Design Properties	4CAS Mechatronic System Design Properties
EP3G7	Claim	All properties required of the Mechatronic System Design have been achieved.	All properties required of the 4CAS Mechatronic System Design have been achieved.
EP3C7	Context	Mechatronic System Design Process	4CAS Mechatronic System Design Process
EP3G8	Claim	The Mechatronic System Design has been defined in compliance with the process	The 4CAS Mechatronic System Design has been defined in compliance with the process
EP3C8	Context	Physically Realised Mechatronic System	4CAS Mechatronic System
EP3C9	Context	Physically Realised Mechatronic System Properties	4CAS Mechatronic System Properties
EP3G9	Claim	Physically Realised Mechatronic System achieves all its required properties	4CAS Mechatronic System achieves all its required properties

Table 41: Pars 3 Symbols

The properties of the *mechatronic technical safety requirements*, *context EP3C3*, as adapted from ISO 26262, are that the requirements are:

- compliant and consistent with the *mechatronic functional safety concept*
- compliant with the *mechatronic system design*
- compliant with the rules of ASIL decomposition

4CAS evidence is not available to support these claims as the contemporaneous reports were not created according to this *Pars* structure.

The claim *EP3G5: All 4CAS Mechatronic Technical Safety Requirements have been defined in compliance with the process* is in relation to the context *EP3C4*. In the case of 4CAS, the work was developed under a QMS based on a process for producing an *E/E system*. The process did include

interfacing with other departments, so this claim is partially addressed. The evidence to support the claim consists of internal audit reports and external audit reports produced because the QMS was externally certified to ISO 9004 under the TickIT scheme (now discontinued).

C.3.2 EP3G6

The claim *EP3G6: The 4CAS Mechatronic System Design achieves all its required properties* relates to the design artefact that specifies the system design as referenced in *EP3C5*. Examples of the 4CAS design documentation were shown in Figure 59 and Figure 60. Other documentation was produced at the time, but this is not shown here.

The properties of the *mechatronic system design, context EP3C6,* as adapted from ISO 26262, are that the design is:

- compliant and complete with regard to the *mechatronic technical safety concept*
- robust against the causes of systematic failures and the effects of systematic faults

4CAS evidence is not available to support these claims as the contemporaneous reports were not created according to this *Pars* structure.

The claim *EP3G8: The 4CAS Mechatronic System Design has been defined in compliance with the process* is in relation to the context *EP3C7*. In the case of 4CAS, the work was developed under a QMS based on a process for producing an *E/E system*. The process did include interfacing with other departments, so this claim is partially addressed. The evidence to support the claim are internal audit reports and external audit reports produced because the QMS was externally certified to ISO 9004 under the TickIT scheme (now discontinued).

C.3.3 EP3G9

The claim *EP3G9: 4CAS Mechatronic System achieves all its required properties* relates to the physical implementation of the system design as referenced in *EP3C8*. For the 4CAS system this is the pneumatic system, and its ECU, fitted to a vehicle.

The properties of the *physically realised mechatronic system, context EP3C9,* as adapted from ISO 26262, are that it:

- is compliant with *mechanical-E/E system interface specification*
- correctly implements the *mechatronic functional safety requirements*, (*EP2C1*)
- correctly implements the *mechatronic technical safety requirements*, (*EP3C2*)
- achieves the *mechatronic safety goals*, (*EP1C4*) when operating as an *item* in a vehicle in the context of the electrical architecture with other controllers.

A wide variety of tests were performed with each having a test specification and producing a test report, all of which provide evidence to support the claim. The details of these are not shown here.

Appendix D Case Study 2: *Pars* Approach Practicality

D.1 Introduction

The purpose of this case study was to evaluate the *Pars* approach to dividing up an engineering development in the context of a mechatronic development. The case study provided an evaluation of contribution 1, presented in Chapter 3 and Chapter 4. The case study sought to ascertain:

- What potential does the approach have for accurately capturing all the information?
- What potential does the approach have to increase overall understanding of the system?
- How practical is the approach?

The case study is based on 4CAS, described in Chapter 4. A qualitative technique of semi-structured interviews was used as the data collection instrument. General questions were asked to get an understanding of what the practitioners thought of the approach. The sample size is small as it is necessarily restricted to staff still in the company who had worked on the project.

D.2 Case Study Design

The case study looked at a single development within one company. The structure of the case study is based on Yin's Case Study Research methodology [195]. According to Yin's classification, the proposed study is a *Type 2: Single-case embedded design*. It is a single-case design because it is capturing *"... the circumstances and conditions of an everyday situation*". It is an embedded design because there are multiple units of analysis; in this case, each person interviewed is a different unit of analysis.

The set of *Partes* used for the case study was a simplified version of that described in Chapter 4 so as to be more closely aligned with actual practice. It was decided to take this approach to make it easier for the participants to relate to a new way of thinking about the system. The set of *Partes* used was:

- *4CAS Mechatronic System*
- *4CAS E/E System*
- *4CAS Mechanical System*

A briefing sheet was written. This initially used Figure 29 from Chapter 3 and Figure 43 from Chapter 4; it also included an *activity diagram* for each *Pars* that showed the inputs and outputs from the *Pars.* The *activity diagram* was based on the generic *Pars* ontology. It was decided to use the *activity diagram,* rather than a direct presentation of the ontology, because most of the participants were unfamiliar with the modelling technique. This was then reviewed by a colleague, who was not part of the case study, to assess how understandable it was. This review led to some simplifications. These included the removal of the figures from Chapter 3 and Chapter 4 and the creation of a single drawing that included the *activity diagram* for each *Pars,* and showed the

cascade of design information from one *Pars* to another, Figure 85. The *Pars* terminology was also removed as it was seen as unnecessary complication

The questions were divided into three groups. The first group concerned Figure 85 in its entirety, questioning how easy it was to understand and whether it accounted for all the documentation. The second group of questions concerned each individual *Pars*, questioning the details of the documentation and the handling of it in terms of decisions, properties, verification and its physical realisation. The third group of questions were general in nature, questioning the overall usefulness and practicality of the approach. The questions are shown in Appendix E.

D.3 Data Collection and Analysis

As mentioned above, the unit of analysis is the individual participant and a total of five participants were interviewed. They were selected by virtue of them having worked on the project. Between them the participants were involved in all of the *Partes* defined for this case study, Table 42.

ID	Role in 4CAS Development	Experience in Role
P1	System Owner	22 years
P2	Mechatronic Technical Specialist	30 years
P3	Control Engineer	15 years
P4	Software Engineer	30 years
P5	Functional Safety Engineer	15 years

Table 42: Case study 2 participants

The study had approval from the Physical Sciences Ethics Committee at the University of York.

The participants were given a briefing sheet to read. This explained: the purpose of the work to extend the functional safety process to include the mechanical system; the division of the subject matter into different *Partes*, with each *Pars* having the same underlying design process and functional safety argument; the purpose of the case study. The participants were also shown the diagram in Figure 85, and this was referred to throughout the interview.

Each person was interviewed separately and the interview lasted between 45 and 90 minutes. The answers given were recorded by hand and transferred to electronic media, i.e. a spreadsheet, within 48 hours of the interview. When transferring the results, errors in grammar and punctuation in the handwritten notes were corrected. The interviews were conducted over a two-week period in March 2018.

The answers from all participants were combined in a single sheet, and for each question positive and negative responses were recorded and key quotes noted. These were then collated under the themes given in the next section.

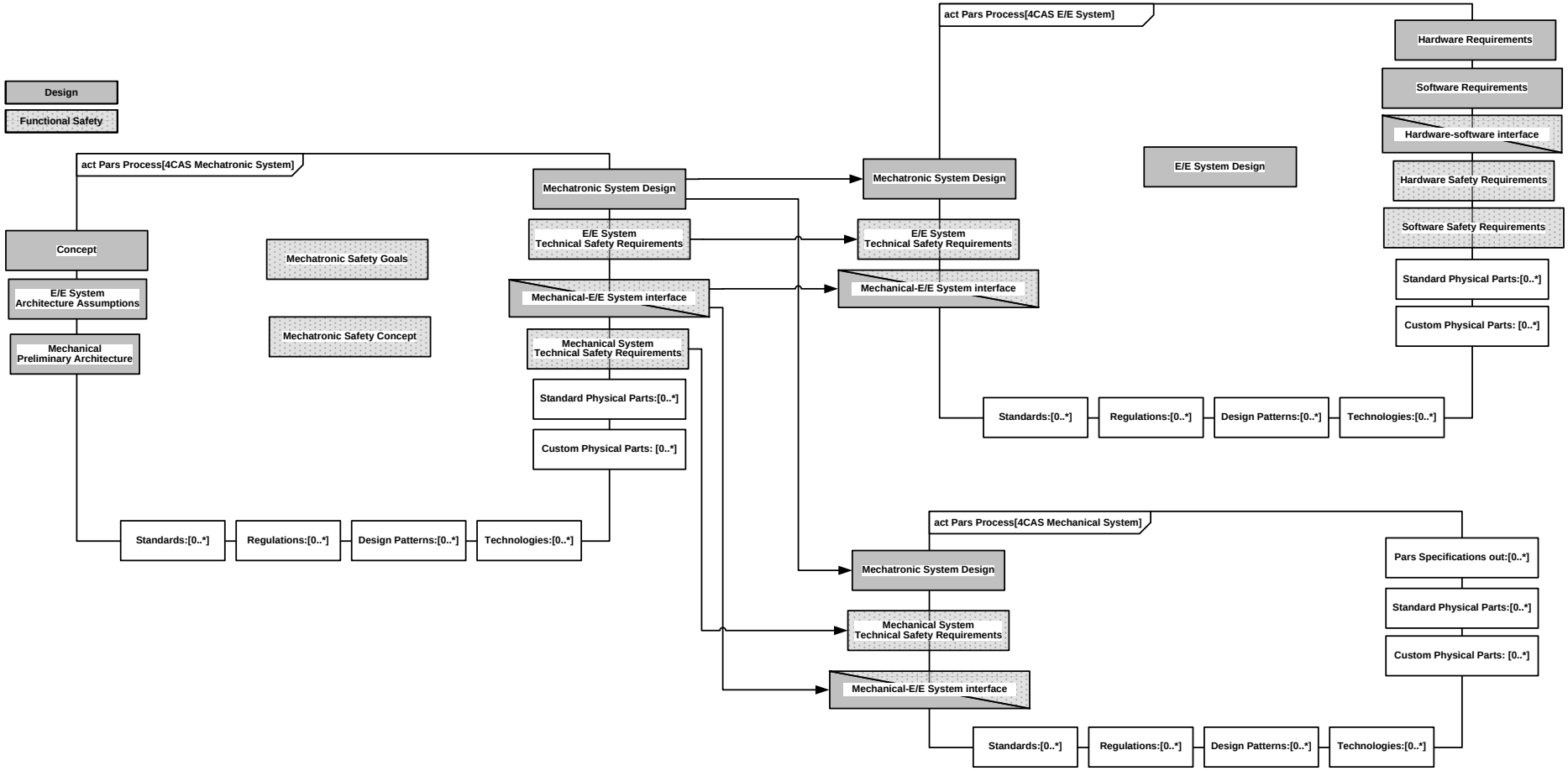

Figure 85: Description of Partes for case study 2

D.4 Case Study Results

The results are presented under the themes of:

- *Pars* Division
- Documentation
- Practicality

Pars Division

The representation of the project as a set of *Partes* with information flowing between them was seen as being representative of the 4CAS development by all of the participants. Showing the link between the *E/E system* and the *mechanical system* highlighted that the system is more than just the software and that the mechanical aspects also contribute to safety. For example, the safe state involves both the *E/E system* and the *mechanical system*. This could help improve the safety argument. It also highlighted the fact that software requirements are often defined by mechanical component constraints; examples include, the need to manage the temperature of the compressor and the fact that the pressure measurement is dependent on the design of both the *E/E system* and the *mechanical system*.

There were some criticisms of the diagram used for the case study. One participant would prefer the systems engineering requirements flow to also be visible so that it was possible to show that each element of a system lifecycle is covered. Also, the diagram does not show the feedback between the *E/E system* and the *mechanical system*; this often leads to changes in requirements and specifications.

Documentation

The activity diagrams included information that corresponded to the blocks of the generic ontology and the participants were able to associate design material in a variety of formats to all of these. One participant commented that it was useful to include the mechanical documentation on the diagram.

The introduction of a *Mechatronic Functional Safety Concept* was seen as being a beneficial addition, as *hazards* are caused by both failures of the *mechanical system* as well as those of the *E/E system*. In practice, the hazard analysis of the 4CAS system had been conducted at a mechatronic level and had consequently produced some new safety requirements for the mechanical design which had not been previously considered.

It was noted that some information was missing from the diagram, for example: calibration, service and manufacturing requirements, problem reports, the electrical network, and the location of physical components.

Practicality

In practice, the *mechatronic Pars* was less formally documented than shown in the diagram and not all of the documentation shown in the diagram was produced. It was also noted that some of the information is the responsibility of the suppliers who historically have not been willing to reveal all their internal information.

Also, the development of the *mechatronic system* and the development of the *mechanical system* are very closely linked; this is not expressed well in the diagram.

When asked about how the process and the evidence produced may be affected by the integrity requirements, one participant was of the opinion that mitigating the risk was more about getting the correct requirements for the interaction between the *mechanical system* and the *E/E system*.

D.5 Discussion

The overall result is positive, and an explicit representation of the development as a *mechatronic system* was seen as an improvement over current practice. The participants were able to engage with the material and readily provide answers to questions. They could relate what had happened during the development, and the material that was produced, to the diagram. This was helped by the fact that the diagram is pitched at a high level of abstraction.

There were some practical concerns about the availability of the documents and the fact that the interplay between the different development streams is not explicitly shown on the diagram. A large amount of mechanical design work was effectively done at the mechatronic level to determine the specification of the mechanical components; this included prototyping.

The cascading of a specification from one *Pars* to another for refinement is perhaps a little artificial, especially as it may well be the same staff who produce both the initial version of the specification and also the final one. Also, requirements often change as a result of feedback between the *Partes*.

Some of these criticisms are of the diagram rather than the approach. The diagram was only created for the purpose of the case study and if carried forward could be improved to address these issues.

To bridge the two worlds of *E/E system* design and *mechanical system* design the approach needs the approval of both sides; it has to be something that both can assent to technically and also something that is not too onerous. The case study shows that the proposed approach has not violated this requirement.

Appendix E Case Study 2 Questions

Name:	
Participant's Background	
Q1	What was your role in the development of the 4CAS System?
Q2	What aspects of 4CAS development were you involved in?
Q3	What previous experience do you have of these types of systems, e.g. number of system, number of years?
4CAS Partes diagram	
Q4	Does the 4CAS *Partes* diagram make sense?
Q5	Can you relate the project documentation to the generic documents used here?
Q6	Is there documentation that does not fit into this scheme?
Q7	Are there any major pieces of documentation missing from the diagram?
4CAS Pars	
Q8	What format did, or could, the documents take?
Q9	How was the completeness of the input documentation assessed?
Q10	What design properties of the input documentation were assessed? What analysis of the input documentation was, or could have been, performed?
Q11	Is it fair to say that the Hazardous Events were derived from the mechatronic inputs?
Q12	What design decisions were made at this point? Standard components Standard design patterns
Q13	Choices: How were these made? Who made them, who approved them? How did the team know that they were the correct decisions?
Q14	Design properties: What design properties were established at this point? How was it decided that these design properties were right / correct / appropriate / acceptable? How could it have been decided?
Q15	Safety properties What safety properties were established at this point? How was it decided that these safety properties were right / correct / appropriate / acceptable? How could it have been decided?
Q16	What design verification, if any, was performed against this level of design?
Q17	Is there any verification that was performed that does not fit in the scheme?
Q18	How was the final design documented? 4CAS system diagram Pneumatic design assumptions Mechatronic modelling, actuators, sensors, BDDs, IBDs
Q19	What does the Mechatronic Safety Concept mean to you?
Q20	How was the completeness of the design documentation with respect to the input documentation and design choices assessed?
Q21	What physical parts were selected or specified at this point?
Q22	How was it established that the physical parts selected or specified would meet the requirements?
Q23	If physical parts were procured or prototyped at this point, how was it established that they met their specification and functional requirements?
Q24	What physical mechanical fitment checks were performed at this point?
General	
Q25	In what way does the partitioning of the material make it easier to comprehend the whole system?
Q26	In what way does the documentation prompt you to think of things that are not as well documented as they should be?
Q27	In terms of a safety argument, does this help?
Q28	Are there artefacts that I have assumed are available which in practice are not available?
Q29	How would you moderate the amount of evidence generated – what would be enough, cf ASIL?
Q30	How would the choice of evidence necessary be affected by the FMEA results?

Appendix F DFMEA Usage Case Study Questions

Q1.1	What products or circumstances will you draw on, in answering these questions?
Q1.2	What company procedure(s) do you use?
Q1.3	How many FMEA do you perform a year?
Q1.4a	How many FMEA do you support a year?
Q1.4b	What is the nature of your support?
Q2.1	What is the purpose of FMEA?
Q2.2	How strongly do you agree with the statement: One purpose of an FMEA is to improve the component being analysed by addressing it most pressing issues? *[Strongly Disagree | Disagree | Neither Agree or Disagree | Agree | Strongly Agree]*
Q2.3	How strongly do you agree with the statement: One purpose of an FMEA is to prevent the product from causing harm? *[Strongly Disagree | Disagree | Neither Agree or Disagree | Agree | Strongly Agree]*
Q2.4	What terms do you prefer to use when discussing issues relating to the product injuring people, e.g. risk, severity, criticality?
Q2.5	What are your completion criteria based on? *[Strongly Disagree | Disagree | Neither Agree or Disagree | Agree | Strongly Agree]*
Q2.5a	Judgement
Q2.5b	Finance/warranty
Q2.5c	Other measure
Q2.6	What is the outcome if it is not done properly? *[Strongly Disagree | Disagree | Neither Agree or Disagree | Agree | Strongly Agree]*
Q2.6a	Warranty
Q2.6b	Critical concerns
Q2.6c	Other
Q2.6d	Examples
Q2.7	How effective do you think this is in achieving its purpose? *[Not at all Effective | Not Very Effective | Partly Effective | Effective | Very Effective]*
Q2.8a	How do you know how effective it is?
Q2.8b	What evidence could you produce to support this?
Q2.9a	How do you decide on the level of confidence you have in the FMEA results?
Q2.9b	What evidence could you produce to support this? E.g. based on experience, level of review, access to design/testing results, etc.
Q2.10	How often is something missed which should have been found? *[Very Frequently | Frequently | Not very Often | Occasionally | Rarely]*
Q2.11	What examples can you give of problems that should they have been, but were not, prevented, by the use of the FMEA?
Q2.12	How do you decide what to investigate and how much to investigate when considering root causes?
Q2.13a	Do you agree that the concept of risk associated with the product causing harm to someone is common across all engineering disciplines, e.g. mechanical, electronic hardware, software?
Q2.13b	Give your rationale for the answer?
Q2.14a	How strongly do you agree with the statement: The effort expended on understanding risk, mitigating risk and gaining confidence in risk mitigation depends on the magnitude of the risk or the criticality of the product failure? *[Strongly Disagree | Disagree | Neither Agree or Disagree | Agree | Strongly Agree]*
Q2.14b	Give your rationale for the answer?
Q3.1	On what basis do you decide the severity score of an effect?
Q3.2	On what basis do you decide the prevention score of an effect?

Q3.3	On what basis do you decide the occurrence score of an effect?
Q3.4	Are actions only for potential effects labelled as YC (critical)?
Q3.5	What happens to potential effects with severity scores of 1 to 8?
Q3.6	What happens if a potential effect labelled YC cannot be eliminated?
Q3.7a	Have you ever, and if so under what circumstances, decided that although a cause is designated with a YC, there is sufficient evidence that it is fully prevented by good countermeasures and detection events?
Q3.7b	What was the evidence?
Q3.8	Of the 5 types of failure modes (No Function, Partial – Over/Under Function, Degraded Over Time, Intermittent Function, Unintended Function), which in your experience:
Q3.8a	Are most often the most appropriate?
Q3.8b	The most difficult to determine?
Q3.9	How do you decide when sufficient countermeasures based on Severity have been identified?
Q3.10	How do you decide when sufficient countermeasures based on Prevention have been identified?
Q3.11	How are the answers to Q3.9 & Q3.10 affected when the effect has been labelled YC?
Q3.12	How often do you find that you have to perform root cause analysis? *[Very Frequently | Frequently | Not very Often | Occasionally | Rarely]*
Q3.13	What are the most common root causes?
Q3.14	When and why are FMEA reviews held?
Q3.15a	How often do you use DMAIC? *[Very Frequently | Frequently | Not very Often | Occasionally | Rarely]*
Q3.15b	Comment
Q3.16a	How often do you use DFSS/DCOV? *[Very Frequently | Frequently | Not very Often | Occasionally | Rarely]*
Q3.16b	Comment
Q3.17	Do you have any examples where an FMEA was performed but there were subsequently issues, e.g. large warranty bill, campaigns, white alerts?
Q3.18	Is there anyone else that you think I should talk to?

List of Abbreviations

4CAS	Four Corner Air Suspension
ADAS	Advanced Driver Assistance System
ALARP	As Low as Reasonably Practical
ASIL	Automotive Safety Integrity Level
BDD	Block Definition Diagram
CAA	Civil Aviation Authority
CENELEC	European Committee for Electrotechnical Standardisation
CFMEA	Concept Failure Mode and Effects Analysis
CPRD	Clinical Practice Research Datalink
DAL	Development Assurance Level
DFMEA	Design Failure Mode and Effects Analysis
DFSS	Design for Six Sigma
DGAC	Direction Générale de l'Aviation Civile (France)
DMAIC	Define, Measure, Analyse, Improve, Control
DSC	Dynamic Stability Control
ECU	Electronic Control Unit
E/E	Electrical/Electronics
EAL	Evaluation Assurance Level
EASA	European Aviation Safety Agency
EEC	European Economic Community
EMC	Electro Magnetic Compatibility
ENSREG	European Nuclear Safety Regulators Group
ERA	European Railway Agency
EU	European Union
FAA	Federal Aviation Authority (USA)
FAR	Federal Aviation Regulations (USA)
FDAL	Function Design Assurance Level
FMA	Failure Mode Avoidance
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode Effects Criticality Analysis
FSC	Functional Safety Concept
FTA	Fault Tree Analysis
HARA	Hazard Analysis and Risk Assessment

IAEA	International Atomic Energy Agency
IATF	International Automotive Task Force
IBD	Internal Block Diagram
ICAO	International Civil Aviation Organisation
IDAL	Item Design Assurance Level
IEC	International Electrotechnical Commission
INCOSE	International Council on Systems Engineering
ISO	International Standards Organisation
KSI	Killed or Seriously Injured
MHRA	Medicines and Healthcare Products Regulatory Agency
MISRA	Motor Industry Software Reliability Association
NASA	National Aeronautics and Space Administration
NHTSA	National Highways Traffic Safety Administration
NRV	National Reference Value
OEM	Original Equipment Manufacturer
OMG	Object Modelling Group
ONR	Office for Nuclear Regulation
OW	Operating Window
PFMEA	Process Failure Mode and Effects Analysis
PMHF	Probabilistic Metric for Random Hardware Failures
PRA	Probabilistic Risk Assessment
QM	Quality Management
QMS	Quality Management System
QRA	Quantitative Risk Assessment
RAMS	Reliability, Availability, Maintainability and Safety
RPN	Risk Priority Number
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive Engineers
SAPs	Assessment Principles for Nuclear Facilities
SIL	Safety Integrity Level
SysML	Systems Modelling Language
TAGs	Technical Assessment Guides
TQM	Total Quality Management
TSC	Technical Safety Concept

UK	United Kingdom
UML	Unified Modelling Language
US	United States
VCA	Vehicle Certification Agency
VDI	The Association of German Engineers
VLSI	Very Large-Scale Integration
WENRA	Western Nuclear Regulators Association

References

[1] R.S.Rivett, "The Challenge of Technological Change in the Automotive Industry," presented at the Safety Critical System Symposium, Bristol, UK, 2012.

[2] R.S.Rivett, "Automotive Regulations," presented at the Safety Critical System Symposium, Bristol, UK, 2013.

[3] "Framework for Road Safety," ed: UK Department for Transport, 2011.

[4] "Safe Car - ADAS Forecast - EU/USR/China," SBD2014.

[5] M. Lu, K. Wevers, and R. van der Heijden, "Technical Feasibility of Advanced Driver Assistance Systems (ADAS) for Road Traffic Safety," *Transportation Planning and Technology*, vol. 28, pp. 167-187, 2005.

[6] A. Forrest and M. Konc, "Autonomous Cars and Society," 2007.

[7] C. Weiß, "V2X communication in Europe – From research projects towards standardization and field testing of vehicle communication technology," 2011.

[8] R. H. Bishop, Ed., *Mechatronics an Introduction*. CRC Press, 2006, p.^pp. Pages.

[9] N. H. T. S. Administration, "Technical Assessment of Toyota Electronic Throttle Control (ETC) Systems," 2011.

[10] H.E.Roland and B.Moriarty, *System Safety Engineering and Management*: John Wiley & Sons, 1983.

[11] D. J. Smith and K. G. Simpson, *Functional Safety, A Straightforward Guide to IEC 61508 and Related Standards*: Butterworth Heinmann, 2001.

[12] IEC, "61508-3: Functional safety of electrical/electronic/programmable electronic safety-related systems. Software requirements," ed, 1998.

[13] ISO, "ISO 26262 Road Vehicles -- Functional Safety," ed, 2011.

[14] A. Kossiakoff, W. N. Sweet, S. J. Seymour, and S. M. Biemer, *Systems Engineering - Principles and Practice*, Second ed.: Wiley, 2011.

[15] K. J. Schlager, "Systems Engineering - Key to Modern Development," *IRE Transactions on Engineering Management*, 1956.

[16] INCOSE. (25/08/2017). Available: http://www.incose.org/

[17] NASA, *NASA Systems Engineering Handbook NASA/SP-2007-6105 Rev1*: NASA, 2007.

[18] ISO/IEC/IEEE, "ISO/IEC/IEEE 15288:2015 Systems and software engineering -- System life cycle processes," ed: ISO, 2015.

[19] R. Stevens, P. Brook, K. Jackson, and S. Arnold, "Systems Engineering - coping with complexity," ed: Prentice Hall Europe, 1998.

[20] I. S. Organisation, "ISO/IEC/IEEE 42010 Systems and software engineering — Architecture description," ed: ISO, 2011.

[21] (29/06/2014). *Zachman International*. Available: http://www.zachman.com

[22] J. A. Zachman, "A framework for information systems architecture," 1987.

[23] Y. Dajsuren, C. M. Gerpheide, A. Serebrenik, A. Wijs, B. Vasilescu, and M. G. J. v. d. Brand, "Formalizing correspondence rules for automotive architecture views," in *ACM Sigsoft conference on Quality of software architectures* Marcq-en-Bareul, France, 2014.

[24] M. Broy, M. Gleirscher, P. Kluge, W. Krenzer, S. Merenda, and D. Wild, "Automotive Architecture Framework: Towards a Holistic and Standardised System Architecture Description," Technical University of Munich2009.

[25] I. Jacobson, *Object-Oriented Software Engineering: A Use Case Driven Approach*: Addison-Wesley, 1992.

[26] (02/04/2018). *UML Open Source Specification Project*. Available: http://www.uml.org/

[27] (23/06/2017). *SysML Open Source Specification Project*. Available: http://www.sysml.org/

[28] M. Fowler, *UML Distilled*: Addison Wesley Longman, 1997.

[29] I. Alexander, "Negative Scenarios and Misuse Cases," in *Scenarios, Stories, Use Cases*, I. Alexander and N. Maiden, Eds., ed: John Wiley & SonsLtd, 2004.

[30] J. M. Carroll, "Five Reasons for Scenario-Based Design," in *International Conference on System Sciences* Hawaii, 1999.

[31] P. Zave and M. Jackson, "Four Dark Corners of Requirements Engineering," *ACM Transactions on Software Engineering and Methodology*, vol. 6, 1996.
[32] M. Jackson, "Problem frames and software engineering," *Information and Software Technology*, vol. 47, 2005.
[33] J. G. Hall, M. Jackson, R. C. Laney, B. Nuseibeh, and L. Rapanotti, "Relating Software Requirements and Architectures using Problem Frames," in IEEE Joint International Conference on Requirements Engineering, 2002.
[34] D. L. Parnas and J. Madey, "Functional documents for computer systems," *Science of Computer Programming*, vol. 25, 1995.
[35] A. v. Lamsweerde and L. Willemet, "Inferring declarative requirements specifications from operational scenarios," *IEEE Trans. on Software Engineering*, vol. 24, 1998.
[36] E. Yu, "Towards modelling and reasoning support for early-phase requirements engineering," in *3rd IEEE Int. Symp. on Requirements Engineering*, Washington D.C, USA, 1997.
[37] B. Nuseibeh, "Weaving Together Requirements and Architectures," *IEEE Computer*, vol. 34, 2001.
[38] D. G. Ullman, *The Mechanical Design Process*: McGraw-Hill International, 2010.
[39] *Mechatronics an Introduction*: CRC Press, 2006.
[40] l. A. F. d. Normalisation, "Mécatronique Vocabulaire," ed, 2008.
[41] D. Bradley, "Mechatronics – More questions than answers," *Mechatronics*, vol. 20, 2010.
[42] D. Shetty and R. A. Kolk, *Mechatronics System Design*: PWS Publishing Company, 1997.
[43] R. Isermann, "Mechatronic System – Innovative Products with Embedded Control," *Control Engineering Practice*, vol. 16, 2008.
[44] C. W. D. Silva, *Mechatronics: An Integrated Approach*: CRC Press, 2005.
[45] M. Follmer, P. Hehenberger, S. Punz, and K. Zeman, "Using SysML in the Product Development Process of Mechatronic Systems," presented at the International Design Conference - DESIGN 2010, Croatia, 2010.
[46] A. Johar and R. Stetter, "A Proposal for the use of Diagrams of UML for Mechatronic Engineering," presented at the International Design Conference - DESIGN 2008, Croatia, 2008.
[47] V. D. Ingenieure, "VDI 2206:2004-06 Design methodology for mechatronic systems," ed: Beuth Verlag, 2004.
[48] G. Pahl, W. Beitz, J. Feldhusen, and K.-H. Grote, *Engineering Design A Systematic Approach*: Springer, 2007.
[49] R. Sell and M. Tamre, "Integration of V-model and SysML for advanced mechatronics system design " presented at the REM2005, France, 2005.
[50] F. Mhenni, J.-Y. Choley, O. Penas, R. Plateaux, and M. Hammadi, "A SysML-based methodology for mechatronic systems architectural design," *Advanced Engineering Informatics*, vol. 28, 2014.
[51] D. Motte, "A Review of the Fundamentals of Systematic Engineering Design Process Models," presented at the International Design Conference - DESIGN 2008, Croatia, 2008.
[52] MISRA, *Guidelines for Safety Analysis of Vehicle Based Programmable Systems*, 2007.
[53] S. O. Hansson, "Seven Myths of Risk," *Risk Management*, vol. 7, 2005.
[54] A. Bicevskis, "Unacceptability of Acceptable Risk," *Search*, vol. 13, 1982.
[55] W. D. Rowe, *An Anatomy of Risk*: John Wiley & Sons, 1977.
[56] D. Gardner, *Risk*: Virgin Books, 2008.
[57] D. Kahneman, *Thinking, Fast and Slow*: Penguin, 2012.
[58] T. Bedford and R. Cooke, *Probabilistic Risk Analysis Foundations and Methods*: Cambridge University Press, 2003.
[59] P. Slovic and E. U. Weber, "Perception of Risk Posed by Extreme Events," 2002.
[60] M. Blastland and D. Spiegelhalter, *The NORM Chronicles*: Profile Books, 2013.
[61] U. Beck, *Risk Society Towards a New Modernity*: Sage, 1992.
[62] A. Elliott, "Beck's Sociology of Risk: A Critical Assessment," 2002.
[63] J. O. Zinn, "Social Contexts and Responses to Risk Network (SCARR)

Literature Review: Sociology and Risk," ESRC Working Paper 2004/1, 2004.
[64] J. Adams, "Risk, Freedom and Responsibility," in *The risk of Freedom, Inst. of US Studies, Senate House*, 1998.
[65] H. J. Otway and D. von Winterfeldt, "Beyond Acceptable Risk: On the Social Acceptability of Technologies," 1982.
[66] D. S. L. Jarvis, "Risk, Globalisation and the State: A Critical Appraisal of Ulrich Beck and the World Risk Society Thesis," 2007.
[67] M. Douglas and A. Wildavsky, *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*, 1982.
[68] C. Hood, H. Rothstein, and R. Baldwin, *The Government of Risk* Oxford University Press, 2001.
[69] G. Majone, "The rise of the regulatory state in Europe," *West European Politics*, vol. 17, 1994.
[70] A. A. Marcus, "Risk, Uncertainty, and Scientific Judgement," ed, 1988.
[71] I. Bartle and P. Vass, "Risk and the Regulatory State - A Better Regulation Perspective," Centre for the study of Regulated Industries2008.
[72] H.W.Lewis, *Technological Risk*: W.W.Norton, 1990.
[73] A. Weinberg, "Science and Trans-Science," *Minerva*, vol. 10, 1972.
[74] V. T. Covello and J. Mumpower, "Risk Analysis and Risk Management: An Historical Perspective."
[75] N. G. Leveson, *Engineering a Safer World*: Massachusetts Institute of Technology, 2011.
[76] O. Renn, "Three decades of risk research: accomplishments and new challenges," 1998.
[77] T. Aven, "Perspectives on risk: review and discussion of the basis for establishing a unified and holistic approach," 2004.
[78] T. Aven, "Safety is the antonym of risk for some perspectives of risk," vol. Safety Science, 2009.
[79] T. Aven, "Why risk acceptance criteria need to be defined by the authorities and not the industry?," *Safety Science*, 2011.
[80] I. Grafjodi, "Application of risk analysis for limitation of consequences of major industrial accidents in the context of Seveso II Directive," 2007.
[81] T. Aven, "The risk concept—historical and recent development trends," 2014.
[82] I. Hacking, "An Introduction to Probability and Inductive Logic," 2001.
[83] T. Aven, "How to define and interpret a probability in a risk and safety setting," 2012.
[84] L. J. Cohen, *The Probable and the Provable*: Oxford University Press, 1977.
[85] C. B. Weinstock, J. B. Goodenough, and A. Z. Klein, "Measuring Assurance Case Confidence Using Baconian Probabilities," 2013.
[86] N. N. Taleb, *The Black Swan*: Penguin, 2010.
[87] T. Aven, "On the meaning of a black swan in a risk context," 2013.
[88] T. Aven, "Practical implications of the new risk perspectives," 2013.
[89] C. J. Wright, *Product Liability - The Law and its Implicatins for Risk Management*: Blackstone Press Limited, 1989.
[90] (05/04/2018). *European Railway Agency*. Available: http://www.era.europa.eu
[91] "Railway safety performance in the European Union 2012," 2012.
[92] "The Railways and Other Guided Transport Systems (Safety) Regulations 2006 (as amended)," ed: Office of Rail Regulation (UK), 2013.
[93] "Commission Decision of 5 June 2009 on the adoption of a common safety method for assessment of achievement of safety targets," ed: European Parliament, 2009.
[94] *Commission Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council*, 2009.
[95] CENELEC, "EN 50126-1:2012 Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS process," ed, 2012.
[96] CENELEC, "EN 50128:2011 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems," ed, 2011.

[97] CENELEC, "EN 50129:2003 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling," ed, 2003.
[98] J. R. Müller, J. Drewes, J. May, and C. Trog, "The Formal Representation of the Safety Case Processes described in the EN 5012x norms," 2009.
[99] (26/06/2014). *International Civil Aviation Organisation*. Available: http://www.icao.int/Pages/default.aspx
[100] (26/06/2014). *Federal Aviation Administration Home*. Available: http://www.faa.gov/
[101] (26/06/2014). *European Aviation Safety Agency*. Available: http://easa.europa.eu/home.php
[102] RTCA, "RTCA Paper No. 234-09/PMC-758. Terms of Reference for Software Joint Special Committee/Working Group Software Considerations in Aeronautical Systems," ed, 2009.
[103] SAE, "ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," ed, 1996.
[104] SAE, "ARP4754A: Guidelines for Development of Civil Aircraft and Systems," ed, 2010.
[105] RTCA, "DO-178C: Software Considerations in Airborne Systems and Equipment Certification," ed, 2011.
[106] RTCA, "DO-254: Design Assurance Guidance for Airborne Electronic Hardware," ed, 2000.
[107] D. Daniels, "Certification in Civil Aviation," presented at the Safety Systems Symposium, Bristol, UK, 2013.
[108] (26/06/2014). *Medicines and Healthcare Products Regulatory Agency* Available: http://www.cprd.com
[109] (26/06/2014). *National Institute for Biological Standards and Control* Available: http://www.nibsc.org/
[110] (26/06/2014). *Clinical Practice Research Datalink* Available: http://www.cprd.com
[111] *Guidance for Manufacturers on Clinical Investigation to be Carried Out in the UK*, M. a. H. P. R. Agency, 2013.
[112] ISO, "ISO 14971:2007 Medical devices - Application of risk management to medical devices," ed, 2007.
[113] (26/06/2014). *US Nuclear Regulatory Commission*. Available: http://www.nrc.gov/
[114] *European Nuclear Safety Regulators Group*. Available: http://www.ensreg.eu/
[115] (26/06/2014). *Office for Nuclear Regulation*. Available: http://www.hse.gov.uk/nuclear/
[116] "Safety Assessment Principles for Nuclear Facilities," ed: HSE, 2006.
[117] (26/06/2014). *Probabilistic Risk Assessment (PRA)* Available: http://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html
[118] NRC, "A Proposed Risk Management Regulatory Framework," ed, 2012.
[119] (26/06/2014). *International Atomic Energy Agency* Available: http://www.iaea.org/
[120] (25/06/2014). *Road safety: Road Safety Action Programme (2003-2010)*. Available: http://europa.eu/legislation_summaries/transport/road_transport/l24257_en.htm
[121] "Global Plan for the Decade of Action for Road Safety 2011-2020," ed: World Health Organisation, 2010.
[122] "Ensuring the Decade is Action," in *Make Roads Safe campaign*, ed, 2010.
[123] "Road Casualty Reduction Strategy for Kent 2014-2020," ed: Kent County Council, 2013.
[124] "Licensed to skill: contributory factors in road accidents: Great Britain 2005 - 2009," Institute of Advanced Motorists2010.
[125] "Reported Road Casualties in Great Britain: 2011 Annual Report ", U. D. o. ransport, Ed., ed, 2012.
[126] M. Ellims, "On Wheels, Nuts and Software," in *9th Australian Workshop on Safety Critical Systems*, 2004.
[127] J. Broughton and J. Knowles, "Providing the numerical context for British casualty reduction targets," 2010.
[128] (2012, 25/06/2014). *Transport Committee - Written evidence from the Royal Society for the Prevention of Accidents*.

[129] UNECE. (25/06/2104). *UNECE World Forum for Harmonization of Vehicle Regulations (WP.29)*.
[130] UNECE, "ECE - 79 Uniform Provisions Concerning the Approval of: Vehicle with Regard to Steering Equipment," ed.
[131] (27/06/2014). *Vehicle Certification Agency*. Available: http://www.dft.gov.uk/vca/index.asp
[132] (27/06/2014). *National Highways Traffic Safety Agency*. Available: http://www.nhtsa.gov/
[133] M. Kuehn, T. Hummel, and J. Bende, "Benefit Estimation of Advanced Driver Assistance Systems for Cars Derived from Real-Life Accidents."
[134] "Code of Practice for the Design and Evaluation of ADAS," Response 3: Preventive and Active Safety Applications Integrated Project Contract number FP6-5070752009.
[135] IEC, " Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)," ed, 2005.
[136] "Convention on Road Traffic," ed. Vienna: United Nations, 1968.
[137] ISO, "ISO/WD PAS 21448 Road vehicles -- Safety of the intended functionality," ed, 2017.
[138] ISO, "TS 16949 Quality management systems. Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations," ed, 2009.
[139] W. A. Shewhart, *Economic control of quality of manufactured product*: New York: D. Van Nostrand Company, 1931.
[140] B. G. Dale, T. v. d. Wiele, and J. v. Iwaarden, *Managing Quality*, Fifth ed.: Blackwell Publishing, 2007.
[141] I. O. f. Standardization, "ISO 9000:2015 Quality management systems -- Fundamentals and vocabulary," ed: ISO, 2015.
[142] A. I. A. Group, "Quality Systems Requirements: QS-9000," ed: Automotive Industry Action Group, 1994.
[143] I. A. T. Force, " IATF 16949:2016 Quality management system requirements for automotive production and relevant service parts organisations," ed: International Automotive Task Force, 2016.
[144] I. O. f. Standardization, "ISO 9000-3:1997 Quality management and quality assurance standards -- Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software," ed: ISO, 1997.
[145] I. T. Association, "TickITplus - Base Process Library ", ed: ITA, 2016.
[146] VDA, "Automotive SPICE Process Assessment / Reference Model," ed: VDA, 2015.
[147] I. O. f. Standardization, "ISO/IEC 15504-5:2012 Information technology -- Process assessment -- Part 5: An exemplar software life cycle process assessment model," ed: ISO, 2012.
[148] K. Yang and B. S. El-Haik, *Design for Six Sigma*: McGraw Hill, 2009.
[149] J. McLinn, "A Short History of Reliability," *Reliability Review: The R & M Engineering Journal*, vol. March 2010, 2010.
[150] J. H. Saleh and K. Marais, "Highlights from the early (and pre-) history of reliability engineering," *Reliability Engineering and System Safety*, vol. 91, 2005.
[151] Patrick D. T. O'Connor and A. Kleyner, *Practical Reliability Engineering*, Fifth ed.: Wiley, 2012.
[152] J. P. King and W. S. Jewett, *Robustness Development and Reliability Growth*: Prentice Hall, 2010.
[153] N. Pascoe, *Reliability Technology*, First ed.: Wiley, 2011.
[154] D. J. Smith, *Reliability Maintainability and Risk*, Sixth ed.: Butterworth Heinemann, 2001.
[155] E. E. Lewis, *Introduction to Reliability Engineering*: Wiley, 1996.
[156] *Military Handbook - Reliability Prediction of Electronic Equipment*: Department of Defense, 1991.
[157] (2006, 15/01/2014). *FARADIP.THREE 4.1*. Available: http://www.technis.org.uk/
[158] T. Aven, "Some Considerations on Reliability Theory and Its Applications," 1988.
[159] SAE, "J1739 Potential Failure Mode and Effects Analysis (Design FMEA), (Process FMEA), (Machinery FMEA)," ed, 2009.

[160] IEC, "IEC 60812: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)," 2006.
[161] W. Denson, "The History of Reliability Prediction," *IEEE Transactions on Reliability*, vol. 47, 1998.
[162] G. H. Ebel, "Reliability Physics in Electronics: A Historical View," *IEEE Transactions on Reliability*, vol. 47, 1998.
[163] J. McLeish and W. Tomczykowski, "An Introduction to Physics of Failure and Reliability Physics Methods," presented at the 2013 Annual Reliability and Maintainability Symposium, 2013.
[164] B. Littlewood and L. Strigini, "Software Reliabilty and Dependability: a Roadmap," 2000.
[165] B. Littlewood, "The Problems of Assessing Software Reliability ....when you really need to depend on it," 2000.
[166] S. Brown, "Probabilistic Reliability vs. Failure Mode Avoidance Methodologies Within the Automotive Industry," presented at the 2004 SAE World Congress, Detroit, US, 2004.
[167] T. P. Davis, "Science, engineering, and statistics," *Appl. Stochastic Models Bus. Ind.*, 2006.
[168] G. Taguchi, S. Chowdhury, and S. Taguchi, *Robust Engineering*: McGraw Hill, 2000.
[169] D. P. Clausing, "Operating Window: An Engineering Measure for Robustness," *Technometrics*, vol. 46, 2004.
[170] I. F. Campean and E. Henshall, "Systems Engineering Excellence Through Design: An Integrated Approach Based on Failure Mode Avoidance," 2013.
[171] E. Henshall and I. F. Campean, "A Systems Approach to the Development and Use of FMEA in Complex Automotive Applications," 2014.
[172] VDA, "Quality Management in the Automotive Industry," in *Quality Assurance in the Process Landscape*, ed: VDA, 2012.
[173] J. Puente, R. Pino, P. Priore, and D. d. l. Fuente, "A decision support system for applying failure mode and effects analysis," *International Journal of Quality & Reliability Management*, vol. 19, pp. 137 - 150, 2002.
[174] W. Gilchrist, "Modelling Failure Modes and Effects Analysis," *International Journal of Quality & Reliability Management*, vol. 10, 1993.
[175] M. Rausand, *Reliability of Safety-Critical Systems*: Wiley, 2014.
[176] A. Birolini, *Reliability Engineering: Theory and Practice*, 4 ed.: Springer, 2004.
[177] T. A. C. (ed), *Reliability-Based Mechanical Design*: Marcel Dekker, Inc, 1997.
[178] B. Bergman, J. d. Mare, S. loren, and T. Svensson, *Robust Design Methodogy for Reliability*: Wiley, 2009.
[179] J. B. P. Baufreton, JL. Boulanger, H. Delseny, JC. Derrien, J. Gassino, G. Ladier, E. Ledinot, M. Leeman, P. Quéré, B. Ricque, "Multi-domain comparison of safety standards," presented at the ERTS-2010, Toulouse, France, 2010.
[180] I. O. f. Standardization, "ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model," ed: ISO, 2009.
[181] S. Toulmin, "The Uses of Argument," ed, 1958/2003.
[182] P. Bishop, R. Bloomfield, and S. Guerra, "The future of goal-based assurance cases," in *International Conference on Dependable Systems and Networks*, Florence, Italy, 2004.
[183] P. Wilson, T. P. Kelly, and J. A. McDermid, "Safety Case Development: Current Practice, Future Prospects," presented at the Annual conference; 12th, Centre for Software Reliability: Safety and reliability of software based systems, Bruges, Belgium, 1995.
[184] T.P.Kelly, "Arguing Safety - A Systematic Approach to Managing Safety Cases," PhD, Computer Science, York, 1998.
[185] G. Community, "GSN Community Standard Version 1," ed: GSN Community, 2011.
[186] I. Habli, I. Ibarra, R. Rivett, and T. Kelly, "Model-Based Assurance for Justifying Automotive Functional Safety," presented at the SAE World Congress, Detroit, Michigan, USA, 2010.
[187] J. Birch, R. Rivett, I. Habli, B. Bradshaw, J. Botham, D. Higham, *et al.*, "A Layered Model for Structuring Automotive Safety Arguments," presented at the 10th European Dependable Computing Conference, Newcastle upon Tyne, UK, 2014.

[188] W. C. Regli, X. Hu, M. Atwood, and W. Sun, "A Survey of Design Rationale Systems: Approaches, Representation, Capture and Retrieval," *Engineering with Computers*, vol. 16, pp. 209-235, 2000.
[189] MISRA. (2016, 19/06/18). *MISRA Bulletin Board - MISRA Safety Case guidelines public review*. Available: https://www.misra.org.uk/forum/viewtopic.php?t=1603
[190] D. Man, "Ontologies in Computer Science," *Didactica Mathematica*, vol. 31, pp. 43-46, 2013.
[191] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, 2004.
[192] L. Bergmans, B. Tekinerdogan, I. Nagy, and M. Aksit, "An Analysis of Composability and Composition Anomalies," 2003.
[193] R. Denning, "Applied R&M Manual for Defence Systems," ed: MoD, 2012.
[194] JLR, "JLR FMEA Handbook Version 3.0 - including Robustness," ed, 2014.
[195] R. K. Yin, *Case Study Research: Design and Methods*, 5 ed.: Sage, 2014.
[196] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, pp. 44-101, 2006.
[197] L. Rambaud, *8D structured problem solving: A guide to creating high quality 8D reports*: Phred Solutions, 2006.
[198] Jan M. Myszewski, "On improvement story by 5 whys," *The TQM Journal*, vol. 25, pp. 371 - 383, 2013.
[199] D. Ward and R. Rivett, "Applying the MISRA Safety Analysis Guidelines in the Management of Functional Safety," presented at the SAE World Congress, Detroit, USA, 2006.
[200] J. Birch, R. Rivett, I. Habli, B. Bradshaw, J. Botham, D. Higham, *et al.*, "Safety Cases and their role in ISO 26262 Functional Safety Assessment," presented at the 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP), Toulouse, France, 2013.
[201] T. R. Devi and V. S. Reddy, "Work Breakdown Structure of the Project," *International Journal of Engineering Research and Applications*, vol. 2, 2012.
[202] T. P. Kelly, "Concepts and Principles of Compositional Safety Cases - (COMSA/2001/1/1) - Research Report commissioned by QinetiQ " 2001.
[203] K. Choudhary and P. Sidharthan, "Failure Mode Effects and Criticality Analysis (FMECA) of Electronic Power Conditioner (EPC)," presented at the 5th International Conference on Reliability, Infocom Technologies and Optimization, Amity University Uttar Pradesh, Noida, India, 2016.
[204] R. S. Pressman, *Software Engineering: A Practitioner's Approach*: McGraw-Hill, 1992.
[205] U. S. D. o. Defense, "MIL–P–1629 : Procedures for Performing a Failure Mode, Effects and Criticality Analysis," ed, 1949.
[206] S. o. A. Engineers, "Design analysis procedure for failure modes, effects and criticality analysis (FMECA). Aerospace Recommended Practice, SAE ARP 926.," ed, 1967.
[207] F. M. Company, "Instruction Manual Process FMEA," ed, 1988.
[208] S. o. A. Engineers, "SAE Reference Manual J1739, Potential Failure Mode and Effects Analysis in Design and Manufacturing," ed, 1994.
[209] R.E.McDermott, R.J.Milulak, and M.R.Beauregard, *The Basics of FMEA*, Second ed.: CRC Press, 2009.
[210] (14/04/2017). *FMEA - FMECA*. Available: http://www.fmea-fmeca.com/types-of-fmea.html