EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
CERN – ACCELERATORS AND TECHNOLOGY SECTOR

CERN-ATS-2009-004

Safety Analysis of the Movable Absorber TCDQ in the LHC Beam Dumping System

Roberto Filippini

Paul Scherrer Institut, The Energy Departments, Risk and Human Reliability Group, Villigen, Switzerland

Jan Uythoven

CERN, Technology Department, Accelerator Beam Transfer Group, Geneva, Switzerland

Abstract

The LHC Beam Dumping System nominally dumps the beam synchronously with the passage of the particle free beam abort gap at the beam dump extraction kickers. In the case of an asynchronous beam dump the TCDQ absorber protects the machine aperture. It is a single sided collimator, positioned close to the beam and it has to follow the beam position and beam size during the energy ramp.

This report assesses the different failure scenarios of TCDQ positioning and their likelihood. The failure probability for the two TCDQ systems together is estimated to be 3.6 E-05 (mean value) for one year of LHC operation. This corresponds to a SIL4 safety level, which is considered sufficient. The three dominant failure modes are highlighted.

The calculated failure probability refers to scenarios that are generated and developed inside the TCDQ system. Potential failure sources not included are the interaction with external systems: the transmission of the start signal to the PLC from a dedicated timing card and the manual optimisation of the TCDQ position by the operator. The sensitivity of the TCDQ system to these failures is also discussed and recommendations to address these vulnerabilities are made.

CERN-ATS-2009-004
01/03/2009

Geneva, Switzerland
March 2009

Table of Figures

Table of Tables

Abbreviations

BIC	– Beam Interlocking Controller
LHC	– Large Hadron Collider
MCS	– Management Critical Settings
PLC	– Programmable Logic Controller
PID	– Proportional Integral Derivate
TCDQ	– Target Collimator Dump Quadrupole

1. Introduction

The nominal filling scheme of the LHC consists of 2808 bunches. Most bunches are separated by 25 ns, but larger beam free gaps exists to allow for the risetime of the injection kickers and a gap of 119 bunches (3 μs) allows for the risetime of the beam dump extraction kickers MKD. In case of synchronisation problems between the RF system and the beam dumping system, a failure in the trigger distribution between the different MKD magnets or in case of erratic firing of one of the MKD kickers, several bunches from the beam are swept across the LHC aperture. The TCDQ is a movable one-sided collimator positioned upstream of superconducting quadrupole Q4 in the beam dump region in IR6 which protects the Q4 and the downstream LHC aperture against an asynchronous beam dump. Two TCDQ systems exist, one for each beam.

To correctly protect the LHC aperture, the nominal position of the TCDQ jaw is at about 8σ distance from the beam centre, where σ is the beam size. The TCDQ position will have to follow the beam during the energy ramp. A movement of several millimetres, with a resolution better than 100 μm, is required. The event of an asynchronous beam dump together with an incorrectly positioned TCDQ can lead to serious damage to the LHC. Details of the TCDQ control system requirements can be found in [1, 2, 3]. The likelihood of having an asynchronous beam dump due to faults internal to the beam dumping systems is about 1 per year [4]. The likelihood of an asynchronous beam dump due to other reasons, like a wrong synchronisation relative to the RF system, has not been quantified but is estimated to be of the some order of magnitude.

The TCDQ position is controlled and supervised by a Programmable Logic Controller (PLC), which applies a PID control to two DC motors. Errors in the position controls, which lead to a wrong positioning of the block, must normally generate an interlock (ILK). The local Beam Interlock Controller (BIC) manages these ILKs and issues a beam dump request. The operator in the control room plays an active role only when the TCDQ is in remote control mode for manual position adjustments.

This study aims at assessing the probability that the TCDQ is not correctly positioned to protect the LHC machine from asynchronous beam dumps. The system failures are modelled by a fault tree. A fault tree supports quantitative probabilistic analysis, and returns insights on principal system vulnerabilities (internal and external).

The report is structured as follows: Section 2 briefly summarizes how safety related issues have been considered during the design process and highlights the safety-related features of the TCDQ and its operational modes. In this section the functioning principles of the TCDQ are also described, together with the scope and limitations. Section 3 describes the modelling and analysis methodology and how it has been applied to this study. The failure model of the TCDQ, with the fault tree of the system, and the data analysis to obtain failure probabilities, is discussed in Section 4. Section 5 summarises the results, their interpretation, and the insights obtained. Finally, the report concludes with a short discussion of the implementation of the study results and provides the outlook for possible future work.

2. TCDQ system description

2.1. Safety considerations during the TCDQ design process

The TCDQ design is not redundant (neither at functional nor at component level) with a few exceptions concerning transmission of the ILK to the Beam Interlock Controller. The two TCDQ systems are each dedicated to one ring. Unlike other systems in the LHC, the TCDQ is not subjected to post-mortem diagnostics. The lack of these measures is compensated by

online supervision of control process quantities, such as the position of the motors, the status of components, the integrity of information (e.g. control set points, motor calibration files). All the supervised quantities are interlocked; so as to trigger a beam dump request in case of detected errors and prevent that failure may lead to unsafe conditions.

The corresponding safety measures for the TCDQ are documented in the TCDQ software specification, control specification and test procedures; see [1, 2, 3].

2.2. TCDQ functioning principles and its operational modes

Three views of the TCDQ system are given: a state transition diagram of TCDQ operations, a description at functional level, and the layout, shown in Figure 1, Figure 2, and Figure 3, respectively.

Figure 1 describes TCDQ configurations and modes during LHC operation. At the reception of the start signal (arm and go), the TCDQ system leaves the ready state and moves to tracking. As long as the beam changes its energy, the TCDQ is in tracking configuration and servo automatic mode. The system moves to a hold configuration and servo mode when the beam energy is fixed. In case of manual adjustment of position, the TCDQ moves to its tracking configuration but in remote mode. ILKs are triggered in case of errors and lead to a beam dump request.

The functional architecture of the TCDQ is represented in Figure 2. The functional description is useful for a global understanding of processes but may hide implementation details that are important for safety assessment. For example, the control and ILK functions are represented as separate functions in this figure although they run on the same CPU.

The system layout at assembly level is shown in Figure 3. The layout shows mapping among functions and components, with their signal paths. For example, the control loop function of motor 1 is implemented in the PLC PID control, the analogue I/O board (output), the motor drive, the DC motor 1, then the potentiometer and again the analogue I/O (input).

The control function and the supervision function of the TCDQ are presented in more detail in the following sections.

2.2.1 PLC control function

A simplified layout of the control loop is given in Figure 3. Each motor is driven by the respective motor drive. The control inputs to the motor drives are calculated in the PLC PID. The 'trajectory' of the TCDQ (position versus time) is calculated by the collimator control system and transmitted to the TCDQ control system via the Management of Critical Settings (MCS). This is translated into set points for the motors. The set points are stored in a table in the PLC CPU [1, 2].

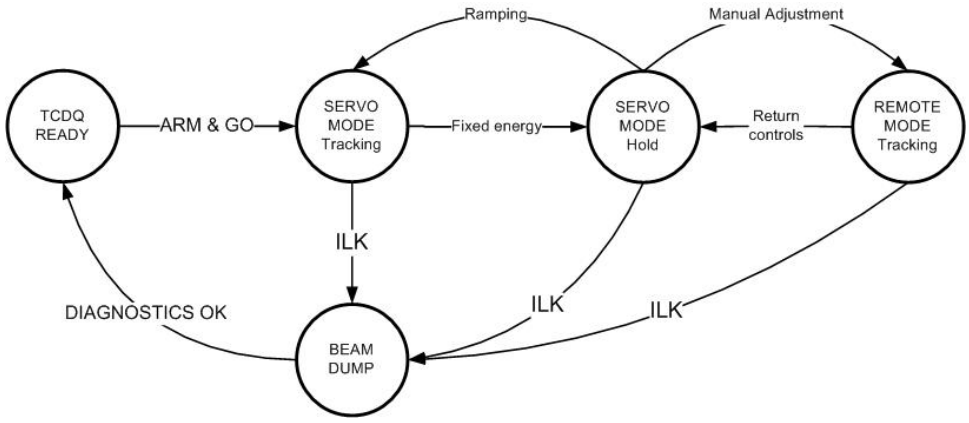

Figure 1: State transition diagram of the TCDQ modes of operation.

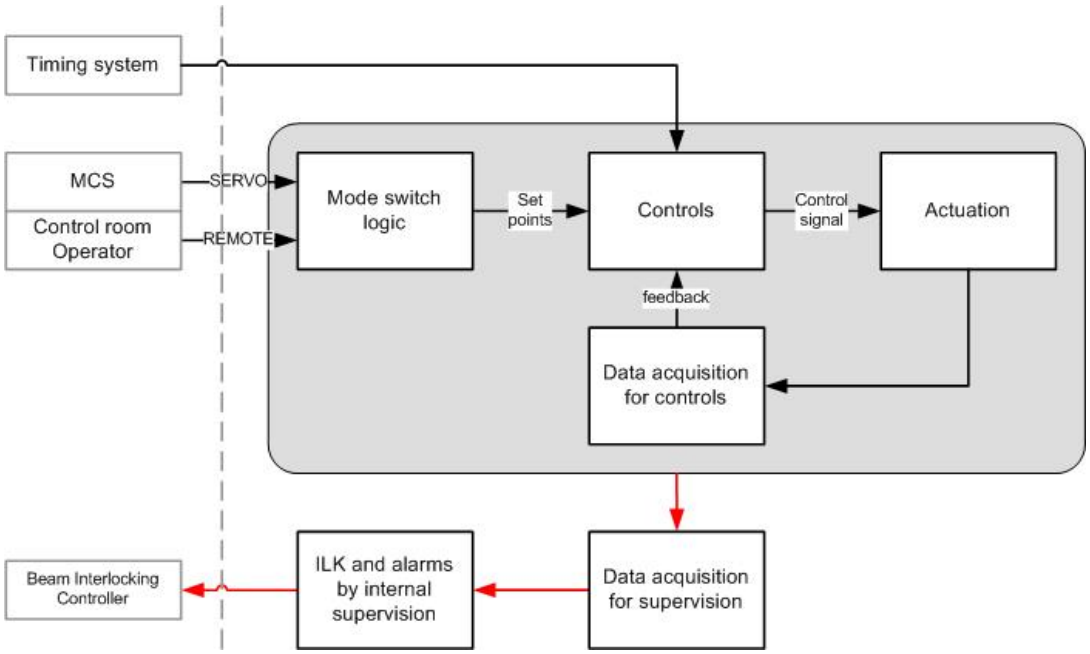

Figure 2: TCDQ functional layout.

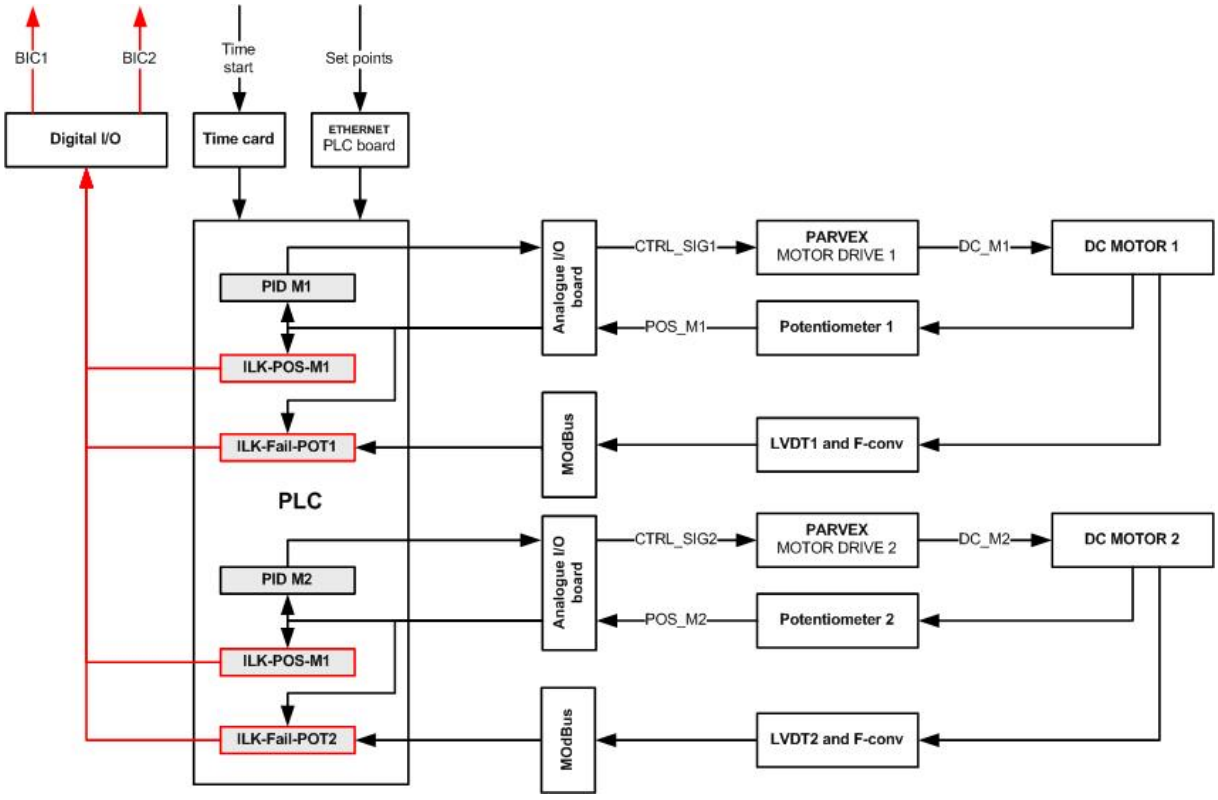

Figure 3: TCDQ layout of control and supervision functions.

The movement of the TCDQ blocks starts when the start signal from the timing system is issued, and received by a timing card via a dedicated transmission. The initial position is the "450 GeV" injection position. The TCDQ is active throughout LHC operation, at LHC injection, LHC ramping and when the machine reaches the full energy for colliding beams. The most demanding configuration for TCDQ, in term of number of components and processes involved, is during position tracking, while ramping and manual adjustments.

During LHC operation with beam, after the start of the fill, the TCDQ is normally in servo automatic mode, controlled by the PLC. In case of fine adjustment of the block position, the operator in the control room may control the TCDQ manually by switching the operation mode into remote. This mode is identical to the servo mode when the TCDQ is in tracking configuration, with the only difference that the set points are provided by the operator in the control room. Manual control of TCDQ, i.e. remote mode, is only possible during the injection phase and with some restriction during a pause of the ramping phase. It is not possible when the LHC is ramping and it should be avoided at top energy. In the present study, it is assumed that adjustments in remote are required once every 10 fills, Ref. [5].

Between two fills the system is moved back to the injection position. This operation challenges the basic functionalities so that it is treated as a functional check for most of TCDQ components. If failures occur in the control or the steering of the block, this is detected before the next fill. The only components not covered by this check are those devices that do not play a role in the controls and steering of the TCDQ, e.g. the supervision functions.

2.2.2 PLC interlock functions

Safe operation of the TCDQ is based on the supervision and interlock function. Many components of the system, which relate directly or indirectly to the TCDQ positioning, are subject to monitoring and verification. Monitoring and verification includes the verification of the correctness of component settings (calibration of motors and PID parameters), verification of the position during the tracking process (independent verification of two motors by error position thresholds, detection of end stop position and emergency stop position) and the status of components and internal self-checking of digital electronics (clock, bus communications, etc.). Interlocks are also generated in case of failure of a power supply and failure in digital transmissions, which are current loops.

The most important supervision function is the TCDQ position read-back. An ILK is triggered if the difference between desired motor position and the actual measurement by the potentiometer exceeds a given threshold. These thresholds are stored in a table in the PLC CPU as they depend on the beam energy. Another ILK is generated in case the motor position measured by the potentiometer and another independent device (LVDT) disagree. Tables with position set points are cross-checked every 10 seconds with the original tables in the MCS and in case of disagreement another ILK is generated. Also the absence of movement of the block to a command is detected and generates an ILK.

All ILKs generated in the PLC go to the digital I/O board and thereby to the BIC. The signal transmission to the BIC is redundant. Position threshold interlocks are modified during the ramping phase. In particular, the time window for the position threshold ILK is augmented in order to track the TCDQ trajectory with a bigger margin of error [1]. This phase is assumed to last 30 minutes and is demanding in term of controls as the position of the TCDQ has to be continuously updated.

2.3. Scope of the study

The study focuses on the TCDQ function to protect the LHC machine. The analysis answers the question: "Given an asynchronous beam dump, what is the probability that the TCDQ is not in the configuration required to protect the LHC machine elements?"

The methodology applied is based on systematically 1) postulating potential initiating events of failure scenarios, 2) identifying the technical and non-technical "defences" against these scenarios, and 3) decomposing the systems and defences into components, their failure modes, and the probabilities associated with these.

The initiating event is the asynchronous beam dump. The mitigation to this event is the function of the TCDQ, protecting the LHC elements. The response of the TCDQ is totally independent to the causes that generate an asynchronous beam dump.

The methodology applied in this study is presented in Section 3. The failure models are discussed in Section 4.

2.3.1 Scope and limitations

The scope credits components that play a role in the TCDQ control and supervision, and the failure of which may results into the misplacement of the TCDQ block. The components included in the scope are:

- two DC motors;

- one diluter block;

- PLC for PID controls (servo mode and remote mode);

- PLC for supervision and interlock generation (several functions);

- PLC self-diagnostics;

- Boards for analogue, digital I/O communication, ETHERNET communications, ModBus communications;

- devices for measuring and validating the motor position (2 potentiometer, 2 LVDT);

- devices for detecting end stop position (1 per motor);

- tables for PID position settings and thresholds, PID parameters and motor calibration.

The list of supervision functions and self-diagnostics is shown in Table 1.

Some of the most important limitations of this TCDQ study concern a few not credited components or functions, simplifications of feedback signals, and coarse modelling of some functions/components or signal paths.

The omitted features or components are some that are demanded only in scenarios that include several simultaneous and independent failure events.

Some supervision functions are not credited. They are the comparison of the LVDT digital and analogue values, the emergency stop switch and the emergency button of the TCDQ. The reason for these omissions stands in the fact these devices take a secondary role in the supervision of the TCDQ. For example, the emergency stop switch is effective only in case the end stop switch does not trigger the TCDQ. Temperature controller and flow controller are not included either.

Some other specific omissions or simplifications are:

1. The operator in the control room is not included in the control chain;

2. MCS, timing system and BIC are not included;
3. Software is not modelled in detail;
4. Component failures that lead to a safe condition are not included.

Point 4 of the list concerns most of digital transmissions, which are 3-wire current loops. For such an electric wiring, a failure at physical level turns into an ILK with the subsequent beam dump. This is true in all failure scenarios with the only exception of a stuck at failure, which is taken into account in the model.

Table 1: Supervision functions accounted in the study

Supervision functions	
Position tracking	Based on error threshold between desired and actual position of motors 1 and 2
Position comparison	Based on comparison of positions of motors 1 and 2 as measured by the potentiometer and LVDT
Position settings	Integrity check of set points in the CPU table with values in the MCS
End stop position	Triggers when the TCDQ reaches the end stop position
Block movement check	Verification that block is not moving
Communication check	Watch dog for ETHERNET communications
Calibration file loading	Detect if the calibration files of motor 1 and 2 are missing at the start of operation
PID parameters loading	Detect if the PID parameters are missing at the start of operation
Motor drive power supply	Power supplies of motor drivers 1 and 2 have failed
ADC	Detect a failure in the ADC converter
Mode of operation	The PLC is functioning in the incorrect mode (remote plus ramping triggers an ILK)
Self diagnostics	
CPU Clock	CPU clock must be 1 kHz
PLC bus	Bus communications between CPU and I/O devices are checked
PLC rack	Detection of general failure of the PLC rack

3. Modelling and Analysis of the TCDQ Failure – the Study Tasks

3.1. Introduction

The safety analysis of the TCDQ verifies whether the system will perform as designed in the postulated scenarios, estimates the likelihood of these failures, and identifies the component

and failure modes that are important to the overall risk. The outcome of this analysis is complementary to the design process: it provides quantitative evidence on the effectiveness of redundancy and diversity to provide barriers and defences against accidents. This information also identifies the components and systems that may deserve particular attention in maintenance and testing. Modifications to the system, its operation, and its maintenance to address the risk-significant vulnerabilities may thus be considered.

3.2. Risk assessment following the IEC 61508 standard

This study is not a risk assessment in the sense of the IEC 61508 standard, which considers the risk without crediting the safety systems. Still, there are good reasons to outline the basics of this methodology, in particular those steps that support in quantitative way the estimation of risk reduction that can be obtained by a protection system. The IEC 61508 safety standard provides three tables to rank risk by consequences and likelihood and thereafter to apportion the correct safety requirements to the protection system, see Ref. [6]. These tables are shown in Figure 4. The last table accounts for the four safety integrity levels, either in term of failure rates or failure on demand. The table with failure on demand is chosen when the risk frequency is about or less than 1 per year, which is the case of the asynchronous beam dump. The apportionment of safety requirement, namely the Safety Integrity Level (SIL), is done by a risk graph method, see Figure 5. Consequences are stated first, then the exposure time (fraction of mission time the system is exposed to the risk), the probability of avoidance and finally the probability of occurrence of the event.

Category	Gravity		Damage	
	Gravity	N. fatalities	Loss(CHF)	Downtime
Catastrophic	Multiple fatalities	> 1	> 100 MCHF	> 3 months
Major	Single fatalities	1	1-100 MCHF	1 week - 3 months
Severe	Non fatal injuries	0.1	0.01 - 1 MCHF	4 hours - 1 week
Minor	Minor injuries	0.01	0 - 10 KCHF	< 4 hours

Frequency	Consequences			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

SIL	SR Control systems	SR protection systems
	Failure rate/h	Prob. of failure on demand
4	$[10^{-9}, 10^{-8}]$	$[10^{-5}, 10^{-4}]$
3	$[10^{-8}, 10^{-7}]$	$[10^{-4}, 10^{-3}]$
2	$[10^{-7}, 10^{-6}]$	$[10^{-3}, 10^{-2}]$
1	$[10^{-6}, 10^{-5}]$	$[10^{-2}, 10^{-1}]$

Figure 4: Risk related tables from IEC 61508 [6].

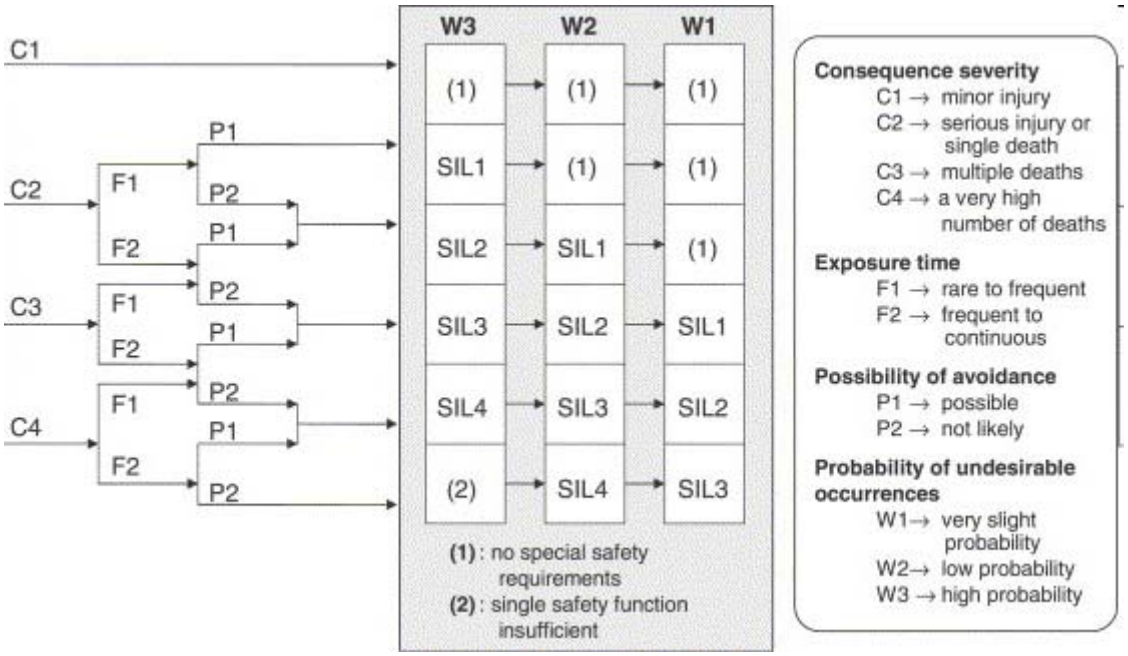

Figure 5: Risk graph method to determine SIL [6]

The risk graph methodology yields a safety integrity level requirement for the TCDQ which is SIL4. This results from the consequence of an asynchronous beam dump which is deemed catastrophic, i.e. 3 months downtime, more than 100 MCHF (C4), the exposure time which is the entire mission time (F2), the probability of avoidance which is null (P2) and the probability of asynchronous beam dump which is low, i.e. 0.4 asynchronous beam dumps per year from one LBDS (W2). It is important to remark that, in term of risk, no distinction is made if an asynchronous beam dump occurs during injection, ramping or top energy phase. The consequences are assumed to be identical, which is a kind of conservative assumption. Other possible sources of asynchronous beam dump (e.g. the RF system) are not included, which is an optimistic assumption. The residual risk likelihood is the product of the probability of failure of the TCDQ multiplied by the frequency of the asynchronous beam dump per year.

The goal of this study is to calculate the probability of failure on demand of the TCDQ.

3.3. System analysis tasks

This is a brief overview of analysis tasks of the TCDQ. They are arranged according to the current practice in Probabilistic Risk Analysis, Ref [7]. These are:

Initiating event analysis considers how accidents can start. More specifically, it identifies the events that require the response of the system to avoid undesired consequences.

In the present case study, the asynchronous beam dump is the initiating event which is an input to the model.

Accident sequence analysis considers the responses to the system to the initiating event.

In this case study, TCDQ can be in the right position or misplaced at the time it is demanded. No adjustments are possible to recover to the right position. This means that the accident sequence consists of just one event: TCDQ is incorrectly positioned and cannot protect the LHC machine elements.

In **Systems Analysis**, the possible causes for the failure of a function required in the scenarios are systematically identified. This is where the failure models are developed. In addition to component failures such as mechanical defects, the systems analysis considers

how the system is checked, repaired and returned to service, in terms of its impact on system failures.

Data analysis refers to the estimation of the frequencies of initiating events (the asynchronous beam dump) and of the probabilities of the "basic events".

Model quantification refers to the failure models which are quantified using the frequencies and probabilities of the events. The results of model quantification include 1) the probability of accident as the combination of the initiating event frequency (the asynchronous beam dump) multiplied by the TCDQ probability of failure, 2) the most probable (dominant) failure scenarios and 3) their contributors. The quantitative contribution of the failure events are measured with importance values. These provide a ranking of the contributions that identify what is important and risk-significant. In addition, when modifications are considered, the importance values provide an indication of how much risk may be reduced by these modifications.

4. Failure model

The failure model of the TCDQ is a fault tree, of which the details are described in the following sections. The description is accompanied by a summary of the analyses necessary to obtain the model.

Section 4.1 documents the models of the TCDQ failure scenarios along the LHC operation scenario. The analyses of the TCDQ in the identified scenarios are addressed in Section 4.2. Section 4.3 discusses the failure events. The data analysis and the resulting probabilities used to quantify the model are presented in Section 4.4 and failure dependencies and common cause failures are in Section 4.5.

4.1. The failure scenario analysis

The TCDQ receives the start signal and keeps adjusting its position with respect to the position and size of the beam. The operation mode is automatic servo (either tracking or holding position) by default. The TCDQ switches to remote mode for manual adjustments of position, which means tracking. The remote mode is inhibited at full energy but it may happen in injection and during the ramping (at a pause). In view of the above, failure scenarios of the TCDQ can be split into failure in position tracking (servo or remote) and failure in position holding. Errors in mode transitions are considered as well. Transition from remote to servo is more critical than servo to remote. The inappropriate servo mode leaves the TCDQ under control of the PLC, while the inappropriate remote leaves the TCDQ basically without control.

A nominal operational scenario will consist of 9/10 fills in servo automatic mode and 1/10 in servo and remote mode [5]. For the fills in servo and remote mode, the fraction of time spent in remote is assumed to be equal to 2 hours,

4.2. Analysis of function/system failures

Fault tree analysis is the systematic, deductive analysis of the possible causes for the failure of functions and systems. The starting point for a fault tree analysis are the success criteria defined for the top event; these consider whether the system functions are within the specified/required range, at the time demanded.

In terms of scope, the fault tree analysis considers:

- the failure modes of the single system components

- the availability of power (electrical, mechanical etc) and other support systems for the components of the system
- the presence and correctness of actuation and control signals, considering the signal paths from logic to actuation elements
- the correct generation and delivery of ILK signals
- integrity of data during transmission, storage, and recall
- the impact of errors during maintenance, testing, return to service, and system configuration
- common cause failures of components within the system or in redundant trains of a system or issued by the same device.

The fault trees lend themselves to be structured in other fault trees, which are made by other fault trees (called transfer gates), and so forth down to the decomposition into basic events. A basic event corresponds to the failure of a component. This the "atomic" block of the fault tree, in which data (e.g. probability, rates, and inspection interval) have to be filled.

A fault tree analysis is performed for the TCDQ system functions, where the top event represents the probability the TCDQ is incorrectly positioned, leaving the LHC elements unprotected from an asynchronous beam dump. The construction of the fault tree follows a top-down approach. The definition of failure is at functional level, which makes it possible to model the failure logic ignoring the implementation details. This is the case of the several supervision functions in the CPU: they are separately modelled with their failure events in the fault tree, though they share the same CPU. This important dependency will appear at the lower component level, with the specification of basic failure events.

Figure 6 shows the fault tree for the failure of TCDQ. The top event is the OR of two branches: 1) TCDQ failure in position tracking and 2) TCDQ failure in position holding. A third branch, which is in OR with the other two, accounts for the human error (manual adjustment) in entering set points or the failure to return operation back to servo. The operator error is a probability of failure on demand, with a demand rate represented by the event REMOTE MODE, equal to 1/10 fills. The TCDQ is in position tracking when the operator performs manual adjustments. The default case study assumes the operator can never fail, which is equivalent to remove contributions of branch three. At any time the TCDQ can be found in position tracking for a certain percentage of the total time and in position holding the rest of time. These figures are in TRACKING and HOLD event and are deduced from estimated operational experience [5].

The differences between the fault trees for position tracking and for holding are in the motors and the block. Motors and block are actuated elements and for this reason they cannot leave the position once they have been driven. For this reason, the branch of the position holding (TCDQ-SERVO-HOLD) is not affected by their failure.

A detailed description of the fault trees with their scope is given in Appendix C, while failure events and failure data can be found in Appendix A and B respectively.

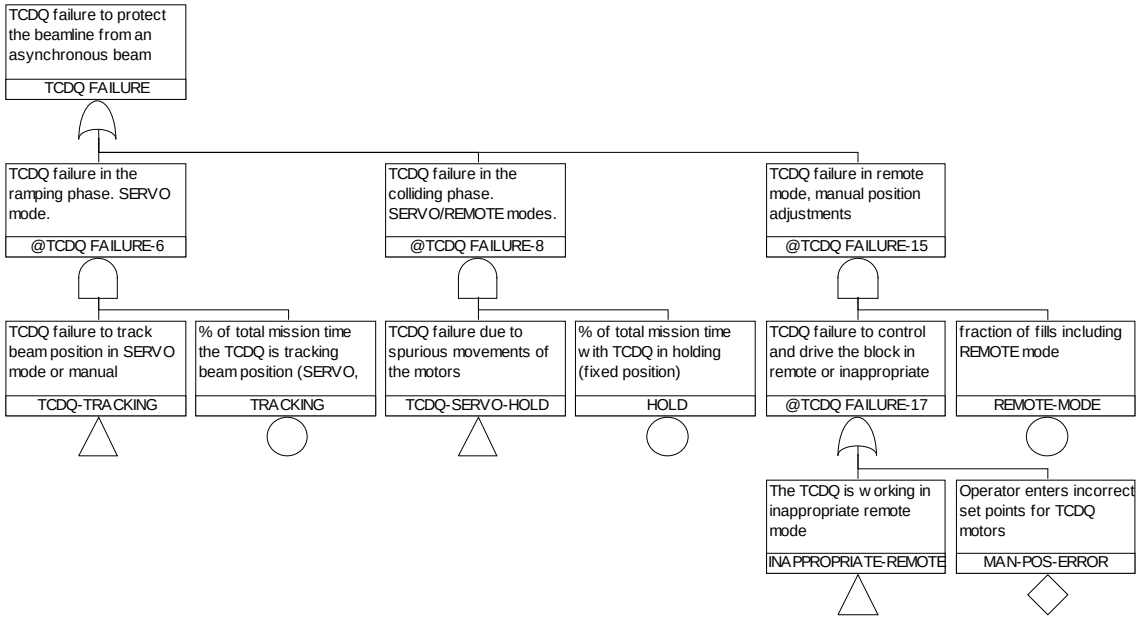

Figure 6: Fault tree of TCDQ failure

4.3. Components and failure events

The basic events representing component failures are identified starting from the point an output is produced or an action performed, (e.g. the generation of the output signal or the response of a final element) back to the sources and including the required support systems. For example, block or motors can fail by not responding to commands, or commands do not reach the motors or they are not correct when generated by the PLC control function. In the same way, ILK signals do not reach the BIC or they are not generated by the PLC interlock function.

In total some 80 basic failure events have been identified. The name of a failure event is identified by a short identifier, which gives information on the component, the function and, if necessary, the signal generated. For example, PID-CONTROL-M1 is the failure of the CPU to calculate the CONTROL input to motor M1.

There are failure modes that turn into a spurious generation of an ILK, then into a beam dump. They only affect the availability of the machine, and for this reason they are not modelled in the safety study. Among these there are:

- errors in control signal generation that move the block into the beam line,
- spurious ILK generated in the PLC supervision logic
- power supply failure (fail safe)
- break-short-false contacts (3-wires current loops in digital communications).

Other failure modes are caught by duplication of signals and comparison (LVDT analogue and digital). They turn as well into a beam dump request and for this reason they are not accounted for in the model.

Other simplifications concern the logic of failure:

- the failure of the positioning of one motor leads to the failure of the TCDQ
- the supervision of TCDQ operation by the operator is not credited

All of these simplifications in the failure models are conservative. The complete list of failure events is given in Appendix A.

4.4. Data analysis – estimation of event probabilities

The level of description in this study is at assembly level and not at the level of components for which statistics of component failure rates exist or they can be deduced by reliability prediction methods. On lack of this specific information, values have been assigned on the basis of previous experience. In particular, failure data set of a previous LHC reliability study (Ref. [4]) has also driven the calculation of the failure data for the TCDQ, in addition to some conservative estimates.

Failure rates are all assumed to be Lognormal distributed, with "error factor" equal to 10. For example, the mean value failure rate of a single output of an Analogue I/O output is 1E-05/h (5^{th} % is 3.75E-07, 95^{th} % is 3.75E-05), while the mean value of the failure rate of the whole board is 1E-06/h (5^{th} % is 3.75E-08, 95^{th} % is 3.75E-06). The mean value of the failure rate of a power converter is assumed to be 1E-05/h. The mean value failure rate of communication (just the output frozen failure event) between two PLC and digital I/O board is 1E-06/h, while this is 1E-04/h if the communication is between the safety switch and the digital I/O. The latter is an example of conservative estimate of the failure rate when the information available is believed insufficient. The list of failure rates with statistics is given in Appendix B.

Data for test and maintenance are defined in Ref. [3]. It is specified that the TCDQ undergoes calibration test at yearly frequency intervals. No special checks are foreseen for the TCDQ during LHC operation and no specific post mortem diagnostics exist. An implicit check on the TCDQ status is assumed between two fills, when the system has to move back to the initial position. This operation challenges almost all components, so it is considered a functional check of many TCDQ components, with the only exception of the ILK functions. Check frequency is every 10 hours, which is the assumed duration of a fill.

4.5. Dependencies and common cause failures

Dependencies are modelled in the fault tree of the TCDQ. A dependency exists when the failures of a set of components depend on the state of another component. For example, the failure of the electronic board implies the failure of all its outputs, which are also modelled as independent failure events.

Common cause failures (CCF) are also modelled. A CCF deals with events or failure mechanisms that can cause failures in identical components of redundant systems simultaneously. A CCF is assigned to a group of components and several CCF groups have been identified in the TCDQ. The list of CCF groups is given in Appendix B.

4.6. Quantification

The analysis and quantification of the fault tree model of the TCDQ is done under the following assumptions:

a) One year of operation of 400 fills, of which 40 are affected by manual adjustments

b) 1 fill is 10 hours

c) Manual adjustment lasts 2 hours

d) Demand rate is 0.4 asynchronous beam dumps per beam, ref. [4]

e) One fill is 2 hours and 15 min in position tracking and 7 hours 45 min in position holding

The analysis of the model must return results in term of average probabilities, which are translated into a SIL figure. Insights on main contributors are also given as minimum cut sets and ranked by component importance.

5. Results and insights

5.1. Overview of results

The fault tree model has been built by using the RISK Spectrum® Software, see Ref. [12].

The tool returns the average probability of failure on demand of the TCDQ per year of LHC operation, 400 fills of 10 hours each, is 1.82 E-05 (5th percentile is 2.7 E-06, 95th percentile is 5.4 E-04). This is 3.64 E-05 for two TCDQs. This figure is independent on the rate of asynchronous beam dumps.

The figure corresponds to a SIL4 (within 1E-05 and 1E-04 probability of failure on demand, see Figure 4). The correctness of external data (e.g. inputs from MCS and timing system) and human errors are not included in the scope of the analysis.

The predominant contributors to the TCDQs failure are:

1) failure of the timing card to transmit start signal to the PLC (60.5%)
2) failure of the PLC with both control and supervision functions (27.5%)
3) failure of the ETHERNET board to transmit correct set points to the PLC (6.0%)

The sets of contributors occur either in position tracking or holding. They are single points of failure of the TCDQ. The other contributors in the control function, motor drive electronics, mechanics etc. are less significant because of internal supervision. Their overall contribution is about 6.0% and individually less than 0.6%, which is a confirmation of the effectiveness of TCDQ supervision during LHC operation.

5.2. Cut sets (failure combinations) and vulnerabilities

Minimal Cut Sets (MCS) are groups of basic events whose occurrence causes the top event of a fault tree to occur. Each MCS represents a specific failure scenario leading to the failure of the TCDQ. The sum of all MCS returns the probability of the fault tree top event.

Minimal cut sets all lead to the same consequences, though they represent different failure scenarios. The dominant (most important) minimal cut sets are shown in Table 2. Four minimal cut sets are about 94.0% of the total probability. The remaining contributors sum to 6.0 % of the total probability and are individually less than 0.6 %. The highest contributors are 3 singletons (single points of failure). The description of the most important minimal cut sets follows.

5.2.1 Minimal Cut Set No. 1: PLC-TIMING-CARD

The largest contribution (with 60.5% of the probability of TCDQ failure) is the PLC-TIMING-CARD failure event, when the TCDQ is in position tracking. The failure scenario corresponds to the failure of the timing card to communicate the start signal to the PLC, as received from the timing system. In other words, the timing card acknowledges the reception of the timing signal to the timing system, but fails to deliver the same signal to the PLC that, for this reason does not track the beam position, leaving LHC unprotected. This failure can only be discovered at the end of the fill.

5.2.2 Minimal Cut Set No. 2 and 3: PLC-CPU-SW

This failure event contributes with 27.5% of the probability of TCDQ failure. It occurs when the PLC CPU fails both with control and supervision, either in position tracking or holding. The PLC runs without changing control inputs to the motors, and this is not detected by the supervision functions. On the basis of available documentation, this failure has been assumed to be undetectable during the LHC operation, while it is discovered at the rearming of TCDQ before next fill.

5.2.3 Minimal Cut Set No. 4: ETHERNET-BOARD

This failure event contributes with 6.0% of the probability of TCDQ failure. It occurs when the Ethernet board fails to transmit the correct set points to the PLC, as received from the MCS. On the basis of the available documentation, this failure has been assumed to be undetectable during the LHC operation, while it is discovered at the rearming of the TCDQ before next fill. The read back of MCS tables is assumed to be ineffective if the failure is such to compare the same incorrect set of data.

Table 2: Minimal Cut Sets of the TCDQ

#	Prob.	%	Failure events		TCDQ configuration
1	1.100E-005	60.5	PLC-TIMING-CARD		TRACKING
2	3.900E-006	21.5	PLC-CPU-SW		HOLD
3	1.100E-006	6.1	PLC-CPU-SW		TRACKING
4	1.100E-006	6.1	ETHERNET-BOARD		TRACKING
5	1.100E-007	0.6	BLOCK FAILURE	PLC-ILK-BLOCKER-SW	TRACKING
6	9.900E-008	0.5	NO-CAL-MOTOR	PLC-ILK-CAL-FILE-SW	TRACKING
7	8.910E-008	0.5	DC-MOTOR2-CAL	PLC-ILK-POS-THR2-SW	TRACKING
8	8.910E-008	0.5	DC-MOTOR1-CAL	PLC-ILK-POS-THR1-SW	TRACKING
9	3.900E-008	0.2	AIO-CTR-MD2	PLC-ILK-POS-THR2-SW	HOLD
10	3.900E-008	0.2	PLC-ILK-POS-THR1-SW	TX-AIO-MD1	HOLD
11	3.900E-008	0.2	MD1-SPURIOUS	PLC-ILK-POS-THR1-SW	HOLD
12	3.900E-008	0.2	PID-CONTROL-M2	PLC-ILK-POS-THR2-SW	HOLD
13	3.900E-008	0.2	PID-CONTROL-M1	PLC-ILK-POS-THR1-SW	HOLD
14	3.900E-008	0.2	PLC-ILK-POS-THR2-SW	TX-PLC-AIO-MD2	HOLD
15	3.900E-008	0.2	MD2-SPURIOUS	PLC-ILK-POS-THR2-SW	HOLD
16	3.900E-008	0.2	PLC-ILK-POS-THR2-SW	TX-AIO-MD2	HOLD
17	3.900E-008	0.2	AIO-CTR-MD1	PLC-ILK-POS-THR1-SW	HOLD
18	3.900E-008	0.2	PLC-ILK-POS-THR1-SW	TX-PLC-AIO-MD1	HOLD
19	1.100E-008	0.1	MD1	PLC-ILK-POS-THR1-SW	TRACKING
20	1.100E-008	0.1	MD2-380PS	PLC-ILK-MD2-SW	TRACKING
21	1.100E-008	0.1	PLC-ILK-POS-THR2-SW	TX-MD2-MOTOR2	TRACKING
22	1.100E-008	0.1	PID-CONTROL-M2	PLC-ILK-POS-THR2-SW	TRACKING
23	1.100E-008	0.1	DC-MOTOR2	PLC-ILK-POS-THR2-SW	TRACKING
24	1.100E-008	0.1	MD2-SPURIOUS	PLC-ILK-POS-THR2-SW	TRACKING
25	1.100E-008	0.1	PLC-ILK-POS-THR1-SW	TX-PLC-AIO-MD1	TRACKING

Other minimal cut sets take a smaller contribution, individually less than 0.6%. They are undetected failure events. Among these, there is the undetected failure of the block (not moving anymore) the undetected failure of the motors and their power converters (MD), the undetected error in communications and the undetected incorrect calibration files. The possibility of undetected inappropriate switching from servo to remote (SWITCH-REMOTE-PLC) is also accounted for in the model, though it is very low in term of probability. Due to their very low contribution, these failure scenarios are not discussed in detail.

It is worth remarking that this set of contributors does not include failure scenarios which develop outside the TCDQ and may jeopardize the functioning (e.g. MCS incorrect set points, missed start signal, and human error in calculating position settings).

The importance results in term of failure events and model parameters are further discussed in the next Section 5.3.

5.3. Importance results

Table 3 shows the most important basic failure events ranked in term of Fussell-Vesely importance (FV) values for the TCDQ unavailability figures. The FV measures the relative contribution of a basic failure event to the overall accident frequency, i.e. the system failure probability without the failure event divided by the system failure probability with the failure event, see also [7]. The higher is the FV the bigger the expected contribution.

Results confirm the importance of PLC-TIMING-CARD, the Ethernet board and the complete failure of the CPU both in controls and supervision. They also show that the TCDQ is more prone to fail while tracking than holding. Software interlocks of position thresholds also come up into the top rank.

Table 3: Importance results

#	Failure event	Prob.	FV
1	TRACKING	2.200E-001	7.620E-001
2	PLC-TIMING-CARD	5.000E-005	6.052E-001
3	PLC-CPU-SW	5.000E-006	2.751E-001
4	HOLD	7.800E-001	2.380E-001
5	ETHERNET-BOARD	5.000E-006	6.063E-002
6	PLC-ILK-POS-THR1-SW	1.000E-003	2.159E-002
7	PLC-ILK-POS-THR2-SW	1.000E-003	2.158E-002
8	BLOCK FAILURE	4.998E-004	6.114E-003
9	PLC-ILK-BLOCKER-SW	1.000E-003	6.050E-003
10	NO-CAL-MOTOR	4.500E-004	5.504E-003
11	PLC-ILK-CAL-FILE-SW	1.000E-003	5.447E-003
12	DC-MOTOR2-CAL	4.050E-004	5.076E-003
13	DC-MOTOR1-CAL	4.050E-004	5.076E-003
14	MASKING-ON	4.200E-003	4.200E-003
15	MD1-SPURIOUS	5.000E-005	2.859E-003
16	MD2-SPURIOUS	5.000E-005	2.859E-003

Table 4 shows the parameters ranked by importance, where the importance measure is the sensitivity. The assumed implicit check of the control function (every 10 hours after the fill) is the most important parameter. Indeed, as it has been already remarked, the TCDQ is supervised during operation and has neither redundant parts nor post mortem diagnostics.

Table 4: Parameters ranked by importance (sensitivity)

#	Parameter	Ti,p,r	Value	Sensitivity
1	CONTROL FUNCTION	Ti	1.000E+001	8.079E+001
2	GENERIC-HW	r	1.000E-005	1.415E+001
3	TRACKING	q	2.200E-001	1.178E+001
4	CPU-SW	r	1.000E-006	4.619E+000
5	ETHERNET	r	1.000E-006	1.637E+000
6	ILK-SW	q	1.000E-003	1.598E+000
7	HOLD POSITION	q	7.800E-001	1.358E+000
8	CAL-FILE	q	4.500E-004	1.169E+000
9	MD-FAILURE	r	1.000E-005	1.069E+000
10	BLOCKER	r	1.000E-004	1.061E+000
11	ANALOGUE-OUT	r	1.000E-005	1.057E+000
12	PID-FAILURE	r	1.000E-005	1.057E+000
13	TX-CPU-ANALOGUE	r	1.000E-005	1.057E+000
14	TX-ANALOGUE-MD	r	1.000E-005	1.057E+000
15	MOTOR-BLOCKER	Ti	1.000E+001	1.051E+000

5.4. Sensitivity analyses: operation, failure data and human error

The TCDQ depends on the correctness of information received from other systems, like the position settings, the start signal, the calibration files and the PID parameters. It also strongly depends on the human error during the adjustment of position settings. These are single points of failure and cannot be discovered by the TCDQ in the present configuration.

This section presents a few analyses, which demonstrate the sensitivity of the TCDQ to the operation scenario, the failure data and the human error.

The sensitivity analysis deals with the operational scenario. In the default scenario, this is assumed to be made of tracking and holding, with the tracking phase being the most critical for the TCDQ. In this sensitivity analysis, the TCDQ is assumed to be always in tracking configuration. The resulting probability of failure on demand of two TCDQ systems is 1.2 E-04, which is SIL3.

The second sensitivity analysis considers a failure data set which is higher by a factor of 10. The resulting probability of failure on demand of two TCDQ systems is 3.6 E-04, which is SIL3.

The sensitivity analysis to the human error is done considering a human error probability equal to 0.01. The TCDQ probability of failure on demand is 2E-03, which is SIl2. Justification about the assumed figure follows.

5.4.1 Sensitivity to human error: justification and insights

A Human Reliability Analysis in which the human-machine interface, procedures, and technical features associated with manual adjustments is included has not been performed. A failure event occurs when the operator fails to adjust the position of the TCDQ in remote mode. This failure scenario is very sensitive to the human error probability.

In this respect, the following assumptions are made:

- Manual adjustments are performed in 1 of 10 fills, or 40 times a year based on the assumed 400 fills per year.
- A manual misconfiguration of the TCDQ always leaves the TCDQ unavailable to protect the LHC in the event of an asynchronous beam dump.
- Multiple adjustments may be performed in a fill that includes a manual adjustment and adjustments are made to both TCDQ motors. In this sensitivity analysis, all adjustments are viewed as a single operation.

The causes of manual misconfiguration may include both "cognitive" errors (incorrect values used in a calculation) and execution "slips" in reading, recall, or manual input:

- miscalculation of the desired TCDQ settings

- error in look-up from a table of previously calculated TCDQ settings

- error in recall of desired settings following look-up

- error in manual input, e.g. a "slip"

Table 5 lists some values from the literature that may be used as a reference. Based on these, 0.01 is selected as a "best" value for the human error probability. This value does not consider factors that could be identified in a detailed analysis of the task, ergonomics, and performance conditions, which could support a lower value.

To justify values of P(misconfiguration /adjustment) below 0.01, a brief task analysis would examine:

- the manner in which the desired manual settings are determined and whether they are calculated during the manual adjustment or previously

- the information used by the operators to determine the desired settings

- how the desired settings are entered (absolute settings, absolute change, percent change, similarity of values for motor 1 and motor 2, scale for motor 1 and motor 2 settings)

- how the operator may perceive the overall system response to the new settings and whether the new settings have the desired effect

- the "aids" (tables, etc.) that would support the operators in determining whether the desired settings are reasonable

- the technical features of the interface that a) could indicate to the operators how the desired settings compare to the previous values set by the MCS for the given LHC state or energy (i.e. current values before the adjustment), b) provide automatic "sanity checks" for the entered settings, or c) could provide limit values (e.g. one-sided) on the input settings.

- how the settings are independently checked and/or confirmed

It can be seen that a number of technical, procedural, aids and administrative features may improve the reliability of manual adjustments. Nevertheless, the error probability of 0.01 corresponds to somewhat less than 1 error for every two years of operation (assuming a total of 40 fills with manual adjustments per year). This may be viewed as a fairly realistic value if there are few opportunities to effectively practice the task. In any case, justifying an error probability at 0.001 or lower will be difficult, even if aids and technical features are provided, given the non-routine character of the task. On the other hand, if the fills involving manual adjustments of TCDQ actually include a series of manual adjustments, the number of opportunities for errors could increase significantly.

Table 5: Methods of HEP and HEP figures

Source	Description	Value
THERP [8]	Initial-screening model Table 20-2 Failure to perform rule-based action correctly when written procedures are available and used, after diagnosis (1) Errors per critical step without recovery factors	0.05 (EF = 10)
	Initial-screening model Table 20-2 (2) Errors per critical step with recovery factors	0.025 (EF = 10)
NARA [9]	Generic Task Type A2 Start or reconfigure a system from the Main Control Room following procedures, with feedback. This would apply if the procedure were to indicate the TCDQ settings to apply. However, it is assumed the staff are determining the TCDQ manual settings on a case-by-case basis, using their experience. TCDQ manual adjustments cannot be considered routine.	1E-3
Kirwan [10]	Human Performance Limiting Values Single operator carrying out task(s), less than optimum ergonomics This is not an estimate but a lower bound for individual performance, representing the error rate under the best possible conditions.	1E-3
ATHEANA [11]	Suggested calibration points for experts (nuclear power plant tasks) The operator(s) would “Infrequently” fail. The level of difficulty is moderately high, such that we should see an occasional failure if all of the crews/operators were to experience this scenario.	~ 0.1
	The operator(s) is “Unlikely” to fail. The level of difficulty is quite low and we should not see any failures if all the crews/operators were to experience this scenario.	~ 0.01
	The operator(s) is “Extremely Unlikely” to fail. This desired action is so easy that it is almost inconceivable that any crew/operator would fail to perform the desired action correctly and on time.	~ 0.001

5.5. Results and SIL

The assessment of residual risk comes from the combination of the probability of failure of the TCDQ multiplied by the frequency of the asynchronous beam dump per year. The overall estimate probability of TCDQ failure is 3.64E-05 which corresponds to a safety level of SIL4. According to the IEC 61508 standard, the calculated SIL4 is adequate to reduce the risk of damaging LHC elements in case of an asynchronous beam dump for both beams, at that rate (0.8/year) and for the assumes consequences (catastrophic).

The result is very sensitive to model assumptions, the failure data and the human error if the operator is included in the control loop. Figure 7 shows the result for the TCDQ in the default case study and the results from sensitivity analysis. The worst SIL is obtained when human error is accounted for in the model.

It is important to remark that results have been obtained under some conservative and some optimistic assumptions. In particular:

- Misconfiguration of the TCDQ, either small or big, always leads to failure
- Asynchronous beam dumps are those generated in the LBDS only
- Rearming cover diagnostics of system components, which are recovered to an as-good-as-new state at every new fill.

The first assumption is conservative, while the second and third assumptions are optimistic. The number of asynchronous beam dumps could also impact on the choice of the SIL table. A number of asynchronous beam dumps equal or higher than 10 per year would suggest the use of the table with failure rates instead of the table with probabilities on demand.

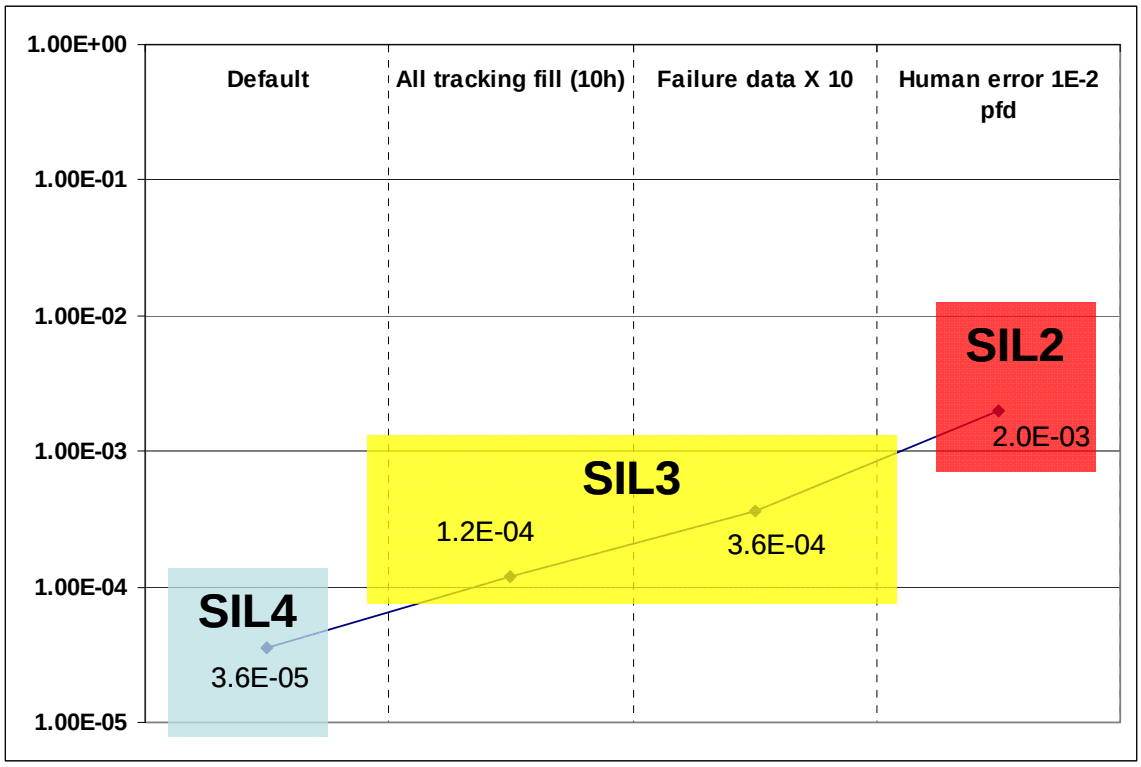

Figure 7: Sensitivity analyses of TCDQ PFD versus operation scenario, failure data and HEP.

5.6. Main insights and modifications based on the results

The safety study of the TCDQ systems returns a low residual risk for the TCDQ failure in case of an asynchronous beam dump. The safety level is SIL4.

The identified system vulnerabilities, the three single points of failure in particular, can be addressed by the following design modifications:

- TCDQ failure of the PLC timing card that receives the start signal: acknowledge the start signal from the PLC which attests the PLC entered the ramping phase.

- TCDQ CPU complete failure at the application level (control functions and supervision functions): make sure this failure is caught by some interlock or implement controls and supervision in two separated PLC.
- TCDQ Ethernet board: make sure incorrect set points transmitted to PLC can be detected in the same PLC
- TCDQ interlock generated by supervision function: check of interlock functionality at regular interval.
- Human error: limiting the modification that the operator may apply by a manual adjustment of position

Among the modifications, the physical separation of control functions and supervision is also recommended in the design of safety critical systems.

The impact of human error on TCDQ operation calls for the analysis of the adjustment tasks, procedures and performance conditions in order to identify defences currently in place and possible improvements.

6. Conclusions and outlook

6.1. Outcome

Based on the IEC 61508 standard, the estimated risk of not protecting the LHC from an asynchronous beam dump, (0.8 per year and catastrophic), leads to the requirement that the TCDQ must meet SIL4.

The analysis has calculated the probability of failure on demand of the TCDQ, while it does not review the SIL-related requirements on design, maintenance and operation of the system.

The result for an assumed default operation scenario, 400 fills, 20% of the time in position tracking and 80% in position holding, is estimated to be 3.64E-5 for the two TCDQs (one per beam). Two major assumptions underlying this value are:

- MCS and timing system inputs to TCDQ are correct
- The system is operated only in servo (automatic) mode with no manual adjustment of TCDQ position

With these assumptions the TCDQs satisfy SIL4.

The TCDQ is designed to cope with the majority of internal failure events, and many of those which are not covered can be discovered in between two consecutive LHC fills. Still, three dominant contributions to TCDQ unavailability are identified:

1. Failure of the PLC timing card to transmit the start signal to the PLC.
2. Failure of the PLC CPU to provide position controls and supervision.
3. Failure of the Ethernet to transmit set points to the PLC.

The three dominant contributions appear to be single points of failure, based on the provided documentation.

A vulnerability to human error exists, if the operator is included in the control of the TCDQ. A list of recommendations has been provided to address and possibly remove the identified vulnerabilities, and obtain a further risk reduction.

6.2. On-going and future work

In future work, the scope of the TCDQ study can be broadened in order to include those parts that were not credited in the analysis. In particular, this may include the generation of the start signal, the correctness of the set-points in the MCS, and the contribution of the human error to the overall risk. The impact of human error is suggested to be the first issue to address due to the dominant contribution in worsening the SIL figure.

Acknowledgements

We wish to thank E. Carlier and C. Boucly for their help in the familiarisation with the system. Our gratitude goes also to Dr. V. Dang for the useful discussion we had with him in the preparation of this work and to V. Mertens for reviewing this document.

References

[1] C. Boucly, Low level software for embedded TCDQ/TCDS control, CERN EDMS document, 15-11-2007, CERN Geneva.

[2] W. Weterings and B. Goddard, Control requirements for TCDS and TCDQ, CERN document, 10-09-2007, CERN Geneva.

[3] VV. AA., Procedures of test: collimator-TCDQ RA63 (4L6 B2), 11-2007, CERN Geneva.

[4] R. Filippini, Dependability analysis of a safety critical system: the LHC beam dumping system at CERN, CERN Geneva 2006.

[5] Jan Uythoven, private communication, 2008.

[6] International Electro-technical Commission IEC, Functional Safety of Electrical-Electronic-Programmable Electronic Safety Related Systems, IEC 61508 International Standard, Geneva, 1998.

[7] Fullwood, R.R., 2000. Probabilistic Safety Assessment in the Chemical and NuclearIndustries. Butterworth-Heinemann,Woburn, Massachusetts, USA.

[8] Swain AD, Guttmann HE (1983). Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington D.C., USA.

[9] Kirwan B, Gibson H, Kennedy R, Edmunds J, Cooksley G, Umbers I (2004), "Nuclear Action Reliability Assessment (NARA): A Data-Based HRA Tool. Proc. 7th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM 7 – ESREL '04), Berlin, Springer-Verlag.

[10] Kirwan B (1994). A Guide to Practical Human Reliability Assessment. New York, CRC Press.

[11] US NRC (2007). ATHEANA User's Guide - Final Report, NUREG-1880, U.S. Nuclear Regulatory Commission, Washington DC, USA.

[12] Risk Spectrum® PSA Professional, 2008. RiskSpectrum Risk Management Software Copyright ©Relcon Scandpower AB 2008.

Appendix A: Failure basic events

Basic failure events are either referring to the output of the component (when an output is not generated) or to the result of action which is the case of a final element that has to stop the beam.

The failure rate model types applied to the Probabilistic Risk Analysis (PRA) basic failure event are those available in the Risk Spectrum® PRA. The complete list includes:

- MR: monitored, repairable component
- PT: periodically tested component
- PD: component with constant probability per demand
- CM: component with constant mission time
- FR: component characterised by occurrence frequency (used for initiating events)
- NR: non-repairable component.

Taking into account the characteristics of the TCDQ operation, two model types are used; the PT and the PD. The PT model uses the failure rate of the component with the inspection/test interval. The PD model uses the probability to fail on demand, which is independent on the assumed inspection/test interval. Probabilities and rates have been deduced by previous analysis on LHC system, see Ref. [4]. Due to the fact description is at functional level and not at component level, the failure modes are apportioned to the assemblies instead of components.

The list of basic failure events is shown in Table 6, accompanied with a short description and the applied model (failure rate or probability on demand). Symbols that represent failure events in Risk Spectrum are 1) circles for basic failure events which do not need any further decomposition, and 2) diamonds for failure events that might be further decomposed. The latter failure events are given more conservative failure rates.

MAN-POS-ERROR and REMOTE-NO-RELEASED, which belong to the human error during manual adjustment of TCDQ position, are also included. These two failure events have been considered in the sensitivity analysis of subsection 5.4.

Table 6: failure events

ID	Description	Model
AIO-CPU-POSM1	Failure of Analogue I/O output feedback signal from potentiometer at motor 1 to CPU	Rate
AIO-CPU-POSM2	Failure of Analogue I/O output feedback signal from potentiometer at motor 2 to CPU	Rate
AIO-CTR-MD1	The control signal CTR-MD1 is not generated at the output of the Analogue I/O board	Rate
AIO-CTR-MD2	The control signal CTR-MD2 is not generated at the output of the Analogue I/O board	Rate
DC-MOTOR1	Breakdown of DC motor 1	Rate
DC-MOTOR1-CAL	Incorrect calibration of motor 1	Probability
DC-MOTOR2	Breakdown of DC motor 2	Rate
DC-MOTOR2-CAL	Incorrect calibration of motor 2	Probability

DIO-BIC-ILK1	ILK1 to BIC stuck at OK at the digital I/O output	Probability
DIO-BIC-ILK2	ILK2 to BIC stuck at OK at the digital I/O output	Rate
DIO-BOARD	Failure of the digital I/O board with all outputs stuck at	Rate
ENDSTOP-OUT-M1	Motor 1 blocked in end stop out position (16.5 mm)	Rate
ENDSTOP-OUT-M2	Motor 2 blocked in end stop out position (16.5mm)	Rate
ENDSTOP-SWITCH-M1	Failure of switch of motor 1 end stop out stuck at open (signal is stuck at OK)	Probability
ENDSTOP-SWITCH-M2	Failure of switch of motor 2 end stop out stuck at open (signal is stuck at OK)	Probability
ETHERNET-BOARD	Failure of the PLC Ethernet board	Rate
ETHERNET-SETPOINTS	Failure of Ethernet to transmit set points to CPU	Rate
ETHERNET-WD	Failure of the Ethernet watch dog	Rate
MASKING-ON	The position threshold are inappropriately masked on	Probability
MD1	Breakdown of PARVEX MD1 (electronics)	Rate
MD1-380PS	Failure of the PARVEX MD1 power converter	Rate
MD2	Breakdown of PARVEX MD2 (electronics)	Rate
MD2-380PS	Failure of PARVEX MD2 power converter	Rate
NO-CAL-MOTOR	Missed calibration file for motors	Probability
PID-CONTROL-M1	Failure of the PID (SW) to calculate the control input to motor 1	Rate
PID-CONTROL-M2	Failure of the PID (SW) to calculate the control input to motor 2	Rate
PID-PARAMETERS	PID parameters are incorrect	Probability
MAN-POS-ERROR	PID set points are not correct for motor 2 as provided by the operator in the control room	Probability
PID-SETPOINTS-MISS	Set points and thresholds are not loaded in the PID	Probability
PID-THR1	Incorrect thresholds for position motor 1	Probability
PID-THR2	Incorrect thresholds for position motor 2	Probability
PLC-BUS-AIO	Failure of BUS-interface between CPU and PLC analogue I/O board	Rate
PLC-BUS-DIO	Failure of BUS-interface between CPU and PLC digital I/O board	Rate
PLC-CLOCK	Failure of PLC clock	Rate

PLC-ILK-AIO-ADC-SW	Failure of SW to generate ILK in case of error in the PLC ADC converter	Rate
PLC-ILK-BLOCK-SW	Failure of SW to generate the ILK in case of no displacement of the TCDQ block	Rate
PLC-ILK-BUS-INTER-SW	Failure of SW to generate the ILK in case of PLC BUS failure	Rate
PLC-ILK-CAL-FILE-SW	Failure of SW to generate ILK in case of absence of calibration file of DC motors	Rate
PLC-ILK-CPU-CLOCK-SW	Failure of SW to generate ILK in case of failure of PLC CPU clock	Rate
PLC-ILKENDSTOP-M1-SW	Failure of software to generate the ILK in case of end stop out position is reached by motor 1	Rate
PLC-ILKENDSTOP-M2-SW	Failure of software to generate the ILK in case of end stop out position is reached by motor 2	Rate
PLC-ILK-LVDT-POT1-SW	Failure of the SW to generate ILK in case of disagreement between LVDT and potentiometer pos of motor1	Rate
PLC-ILK-LVDT-POT2-SW	Failure of the SW to generate ILK in case of disagreement between LVDT and potentiometer pos of motor2	Rate
PLC-ILK-MD1-SW	Failure of SW to detect the failure of the MD1 PARVEX power converter	Rate
PLC-ILK-MD2-SW	Failure of SW to detect the failure of the MD2 PARVEX power converter	Rate
PLC-ILK-MODE-SW	Failure of SW to generate the ILK in case of incorrect mode of operation	Rate
PLC-ILK-PID-FILE-SW	Failure of SW to generate the ILK in case the PID setting file is not loaded	Rate
PLC-ILK-POS-THR1-SW	Failure of SW to generate the ILK in case the threshold position of motor 1 is exceeded	Rate
PLC-ILK-POS-THR2-SW	Failure of SW to generate the ILK in case the position threshold of motor 2 is exceeded	Rate
PLC-ILK-RACK-SW	Failure of SW to generate ILK in case of failure of the PLC rack	Rate
PLC-RACK	Failure of the PLC rack	Rate
PLC-TIMING	Failure of the PLC timing card	Rate
POT-M1	Failure of potentiometer to calculate the position of motor 1	Rate
POT-M2	Failure of potentiometer to calculate the position of motor 2	Rate
REMOTE-NO-RELEASED	The operator fails to return control mode into servo	Probability
SWITCH-REMOTE-PLC	The PLC switches to REMOTE mode	Probability
TIMING-START	Failure of timing system to send start signal to PLC	Rate

TX-AIO-CPU-POSM1	Failure of transmitting the motor 1 position feedback from the analogue I/O board to the PLC CPU	Probability
TX-AIO-CPU-POSM2	Failure of transmitting the motor 2 position feedback from the analogue I/O board to the PLC CPU	Probability
TX-AIO-MD1	TX failure of CTR-MD1 signal from Analogue I/O board to Motor drive 1	Probability
TX-AIO-MD2	TX failure of CTR-MD2 signal from Analogue I/O board to Motor drive 2	Probability
TX-DIO-BIC1	TX failure of TCDQ ILK signal 1stuck at OK at the BIC input	Probability
TX-DIO-BIC2	TX failure of TCDQ ILK signal 2 stuck at OK at the BIC input	Probability
TX-ENDSTOPM1-DIO	Failure of transmission between end stop safety switch and digital I/O board, signal stuck at OK	Probability
TX-ENDSTOPM2-DIO	Failure of transmission from end stop switch motor2 to digital I/O, signal stuck at OK	Probability
TX-MD1-MOTOR1	Failure in the cabling between motor drive 1 and motor 1	Probability
TX-MD2-MOTOR2	Failure in the cabling between motor drive 1 and motor 1	Probability
TX-PLC-AIO-MD1	TX failure of CTR-MD1 signal from PLC (control function) to the Analogue I/O board	Probability
TX-PLC-AIO-MD2	TX failure of CTR-MD2 signal from PLC (control function) to the Analogue I/O board	Probability
TX-POTM1-AIO	Failure of transmission of position feedback motor 1 from potentiometer to Analogue I/O board	Probability
TX-POTM2-AIO	Failure of transmission of position feedback motor 2 from potentiometer to Analogue I/O	Probability

Appendix B: Failure data

This appendix presents the failure data for basic failure events and CCF used for the safety analysis.

Failure rates

Failure rates are collected from literature. Most popular databases are the Military Handbook 217F, the IEC TR 62380 and the SINTEF reliability prediction method for safety instrumented systems. They all provide reliability models, which calculate the statistics on the component failure rate with respect to several parameters (temperature, operating conditions, etc). In the case studied, by sake of simplicity, some approximations are made to get a conservative estimate of the failure rate. In TCDQ, failure events mainly refer to assemblies, instead of components, so statistics are not directly available neither they can be easily deduced without the support of more detailed documentation. Results from previous LHC reliability studies have also been used to a certain extent [4] and certain failure rates have been slightly overestimated. It is important to remark that the failure rate values are used in combination with the assumed functional test of the TCDQ before the re-arming.

Table 7 shows the list of failure rates per hour. Each quantity is lognormal distributed, with the mean value, 5th and 95th percentiles corresponding to an error factor 10. Specific failure rates are: electronics boards are 1E-06/h, power converters are 1E-05/h, mechanics are 1E-04/h, short communications are 1E-06/h, long communications are 1E-05/h, errors in the PID reference files are all 1E-05/h, and so on. Some of the failure rates (mainly digital boards) correspond to a precise failure mode, which is specified in the description field. Other failure rates (mainly analogue boards) are more general.

Table 7: Failure rates

ID	Description	Mean	Dist.type	Median	5th perc.	95th perc.
ANALOGUE-BOARD	Failure of the analogue board	1.00E-06	Lognormal	3.75E-07	3.75E-08	3.75E-06
ANALOGUE-OUT	Failure of analogue board output (stuck at)	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
BLOCK	Failure of the block to move	1.00E-04	Lognormal	3.75E-05	3.75E-06	3.75E-04
DC-MOTOR	Failure of the DC motor to move	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
DIGITAL-BOARD	Failure of the digital board (stuck at)	1.00E-06	Lognormal	3.75E-07	3.75E-08	3.75E-06
DIGITAL-OUT	Failure of a digital board output stuck at	1.00E-06	Lognormal	3.75E-07	3.75E-08	3.75E-06
ETHERNET	Failure of the Ethernet board and communications (incorrect outputs)	1.00E-06	Lognormal	3.75E-07	3.75E-08	3.75E-06
GENERIC-HW	Failure of generic HW component	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
LVDT	Failure of LVDT and PML 1000 and Power supply	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05

MD-FAILURE	Failure of motor drive power converter	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
MD-MOTOR	Motor drive failure (internal) to drive motor	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
MOTOR-STUCK	Motor stuck at the end switch position	1.00E-04	Lognormal	3.75E-05	3.75E-06	3.75E-04
PID-FAILURE	Failure of PID to generate the correct control signal	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
PID-PAR-ERROR	Error in the calculation of PID parameters	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
PLC-BUS	Failure of internal bus	1.00E-06	Lognormal	3.75E-07	3.75E-08	3.75E-06
PLC-CLOCK	PLC clock failure	1.00E-06	Lognormal	3.75E-07	3.75E-08	3.75E-06
PLC-RACK	Failure of the PLC rack	1.00E-06	Lognormal	3.75E-07	3.75E-08	3.75E-06
POTENTIOMETER	Failure of potentiometer to measure position	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
SETPOINT-ERROR	Error in the calculation of set points for PID	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
SPURIOUS-MODE-SWITCH	Spurious HW failure: TCDQ mode is changed inappropriately	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
TX-ANALOGUE-CPU	Transmission failure from analogue board to PLC CPU	1.00E-06	Lognormal	3.75E-07	3.75E-08	3.75E-06
TX-ANALOGUE-MD	Transmission failure analogue board to motor drive	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
TX-CPU-ANALOGUE	Transmission failure CPU to analogue IO board	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
TX-CPU-DIGITAL	Transmission failure CPU to digital IO board	1.00E-06	Lognormal	3.75E-07	3.75E-08	3.75E-06
TX-DIGITAL-BIC	Transmission failure from digital IO board to BIC	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
TX-MD-MOTOR	Transmission failure motor drive to motor	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
TX-POT-ANALOGUE	Transmission failure potentiometer to analogue IO board	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
TX-START-TIMING	Transmission failure of the start signal	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05

Probabilities on demand

The list of probabilities on demand in the TCDQ model is shown in Table 8. Again, the sample distribution is the Lognormal with 10 as error factor. The failure events with a probability on demand occur when the component is challenged to perform an action just at the time this is demanded. These failure events do not depend on the time between two demands, and because of that they are considered constant probabilities. When applicable, the model of calculation is an average probability = $\lambda T/2$, where λ is the failure rate and T is the mission time, 4000 hours. For example, on lack of periodical checks, the software that implement the supervision function and trigger ILK can be assumed to fail with a rate of 1E-06/h, which multiplied by 4000/2 = 2000 h makes 2E-03. Some probabilities are multiplied by a factor 4.5 and this is done to compensate the fact they are multiplied by 0.22 in the tracking branch, the figure that takes into account the fraction of time spent in tracking configuration.

Table 8: Probabilities on demand

ID	Description	Mean	Dist.type	Median	5th perc.	95th perc.
CAL-FILE	Probability of making a bad calibration	1.00E-04	Lognormal	3.75E-05	3.75E-06	3.75E-04
ELECTR-ON-DEMAND	Failure of electronics components which implement supervision	1.00E-04	Lognormal	3.75E-05	3.75E-06	3.75E-04
END-SWITCH	Failure of end switches	4.50E-04	Lognormal	3.75E-05	3.75E-06	3.75E-04
ILK-SW	Probability the ILK function does not issue the ILK	1.00E-03	Lognormal	3.75E-04	3.75E-05	3.75E-03
OP-ERROR	Human error affecting TCDQ control function	1.00E-02	Lognormal	3.75E-03	3.75E-04	3.75E-02
PID-PARAM	PID parameters are incorrect	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
POS-SET-INCORRECT	Probability of having incorrect settings	1.00E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
POS-SET-MISSING	Probability position settings are missed	4.50E-05	Lognormal	3.75E-06	3.75E-07	3.75E-05
TX-NOTESTED	TX which are not tested, or challenged at every fill	1.00E-04	Lognormal	3.75E-05	3.75E-06	3.75E-04

Other data

Other data for the analysis are the fractions of time the system spends in tracking position, holding position and the fraction of fills that are affected by manual adjustments. They are shown in Table 9.

Table 9: Fraction of time used to model contributions from tracking and hold branches and human error

ID	Description	Mean	Dist.type	Median	5th perc.	95th perc.
HOLDING	Probability the system is in servo mode	7.8E-01	None	7.8E-01	7.8E-01	7.8E-01
REMOTE-MODE	Probability the system is in remote mode	1.00E-01	None	1.00E-01	1.00E-01	1.00E-01
TRACKING	Probability the system is in servo mode	2.2E-01	None	2.2E-01	2.2E-01	2.2E-01

Common cause failures

All CCFs are modelled with a beta factor, which is assumed to be 0.1 for all CCF sets. This value is bigger with respect to the suggested value that one can find in reference manual used to assess risk for safety critical systems, for example the SINTEF (Reliability Prediction Method). It is important not to confuse CCF with dependencies. CCFs are only failure modes that affect at the same time two or more trains of redundancy. The list of CCF sets accompanied by a short description is shown in Table 10.

Table 10: CCF sets

ID	**Description**	**CCF model**	**Failure events**
BUS-IO	CCF of BUS to I/O communications	Beta factor	PLC-BUS-AIO PLC-BUS-DIO
CAL-FILE	CCF in calibration file	Beta factor	DC-MOTOR1-CAL DC-MOTOR2-CAL
DIGITAL	CCF of digital board outputs	Beta factor	DIO-BIC-ILK1 DIO-BIC-ILK2
TX-DIG-IO	CCF of transmissions from digital IO board	Beta factor	TX-DIO-BIC1 TX-DIO-BIC2

Appendix C: Fault trees

This appendix describes the fault trees of the TCDQ. The description is given in term of scope, with the list of components (systems) that contribute to the failure of the top event.

TCDQ FAILURE

The scope of the fault tree of Figure 6 consists of two branches, plus the human error branch, included in the sensitivity analysis. The description of the fault tree is in Table 11.

Table 11: Failure events of the TCDQ failure fault tree.

Top event ID	Top event description	Systems and components modeled	Functions involved
TCDQ TRACKING	Models the failure in automatic (or remote) mode of the TCDQ when tracking beam position. Failure may be in the block to move into the desired position due to a mechanical failure, a failure of motor 1 or motor 2 or a failure in the control electronics. Supervision and ILK functions are included.	TCDQ block Motor 1 and 2 Motor drive	Block actuation
		PLC CPU Bus communications Analogue I/O ETHERNET Set points table Timing card	Calculation of control signal and transmission to motor 1 and 2
		PLC CPU Bus communications Analogue I/O Digital I/O ETHERNET Threshold table Potentiometer 1, 2 LVDT 1, 2	ILK function for block failure, position threshold and feedback comparison for motor 1 and 2 on the basis of position set points
TCDQ SERVO-HOLD	Models the failure in automatic servo mode of the TCDQ to stay in the calculated position. Failure may be in the power converter of motor 1 and 2 and control electronics (spurious controls). Supervision and ILK functions are included.	Motor drives	Block actuation
		PLC CPU Bus communications Analogue I/O ETHERNET Op set points Timing card	Calculation of control signal and transmission to motor 1 and 2 on the basis of operator set points
		PLC CPU Bus communications Analogue I/O Digital I/O ETHERNET Threshold table Potentiometer 1, 2 LVDT 1, 2	ILK function for block failure, position threshold and feedback comparison for motor 1 and 2

MAN-POS-ERROR	Operator enters incorrect set points to TCDQ motors	Operator	Manual adjustment of TCDQ position
INAPPROPRIATE REMOTE	Models the possibility of working in the inappropriate remote mode when the system should be in servo mode.	Operator PLC	Release to servo ILK incorrect mode det.

TCDQ-TRACKING

The scope of the fault tree consists of the blocker and the two control loops (in servo mode) of DC motor 1 and DC motor 2, with the respective power converters, computation of control inputs by PID, feedback signals and position supervision. The tree is built tracking back the signal from the final element actuation (the TCDQ block) back to the actuator and the source of the control signal in the PLC. Failures of signal transmissions are included too. The fault tree is shown in Figure 8, with description in Table 12.

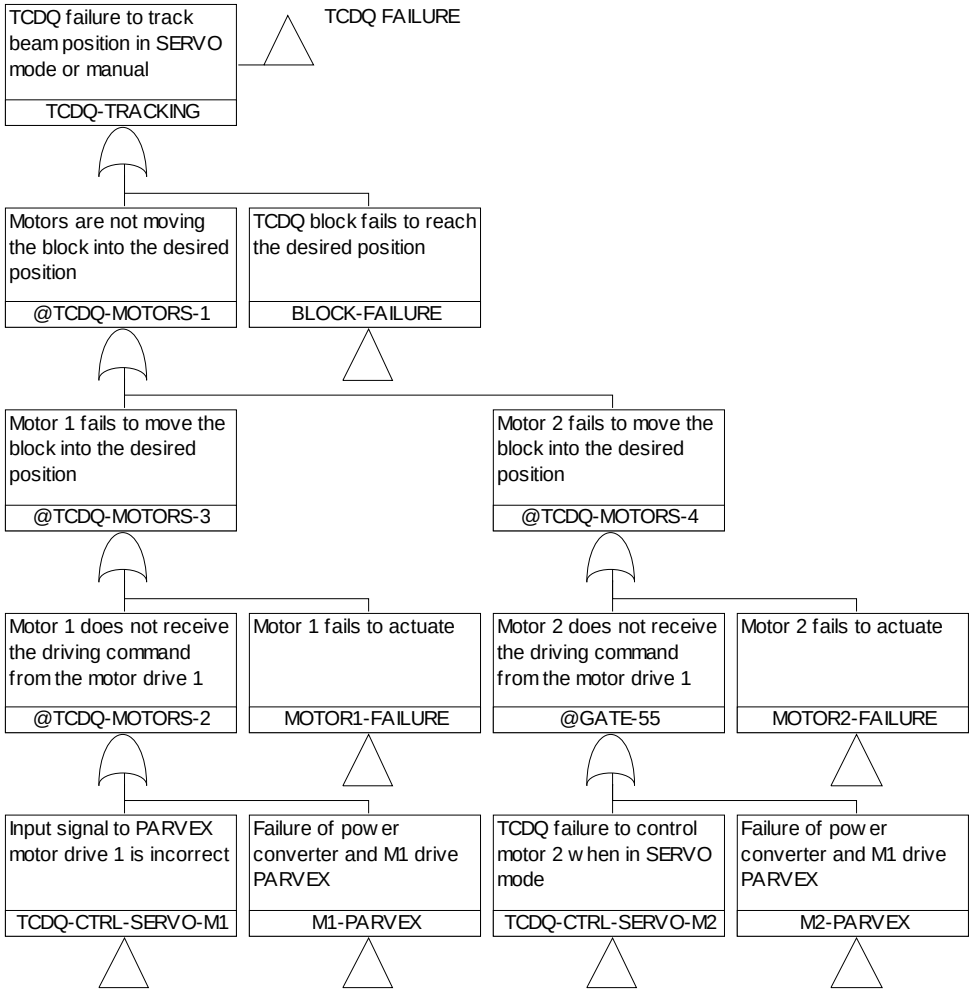

Figure 8: Fault tree of the TCDQ in position tracking

Table 12: Failure events of the fault tree TCDQ-TRACKING

Top event ID	Top event description	Systems and components modeled	Functions involved
BLOCK FAILURE	Models the failure of the block to move in the desired position due to a mechanical failure	TCDQ block PLC CPU Digital I/O board	No block movement ILK
TCDQ-CTRL-SERVO-M1	Models the failure of PLC control function to generate and transmit the correct command to DC motor 1	PLC CPU Bus communications Analogue I/O ETHERNET Set points Timing card	Calculation of control signal and transmission to motor 1
		PLC CPU Bus communications Analogue I/O Digital I/O ETHERNET Threshold table Potentiometer 1 LVDT	ILK function for position threshold and feedback comparison for motor 1
TCDQ-CTRL-SERVO-M2	Models the failure of PLC control function to generate the correct command to DC motor 2	PLC CPU Bus communications Analogue I/O ETHERNET Set points Timing card	Controls calculation and transmission to motor 2
		PLC CPU Bus communications Analogue I/O Digital I/O ETHERNET Threshold table Potentiometer 2 LVDT	ILK function for position threshold and feedback comparison for motor 2
MOTOR1-FAILURE	Models the failure of DC motor 1 to actuate due to mechanical failure or incorrect calibration	DC motor 1 Calibration file 1 End stop switch 1 PLC CPU Digital I/O board Pos. threshold file 1 Calibration file 1	Motor 1 actuation Position threshold 1 ILK End stop 1 ILK No cal. File ILK

MOTOR2-FAILURE	Models the failure of DC motor 2 to actuate due to mechanical failure or incorrect calibration	DC motor 2 Calibration file 2 End stop switch 2 PLC CPU Digital I/O board Pos. threshold file 2 Calibration file 2	Motor 2 actuation Position threshold 2 ILK End stop 2 ILK No cal. File 2 ILK
M1-PARVEX	Models the failure of the motor1 power converter (PARVEX 1) to drive motor 1	MD1 PARVEX electronics MD1 power supply PLC CPU Digital I/O Pos. threshold file 1 Power cabling	Motor 1 driving Position threshold 1 ILK PS MD1 ILK Power cabling
M2-PARVEX	Models the failure of the motor1 power converter (PARVEX 2) to drive motor 2	MD2 PARVEX electronics MD2 power supply PLC CPU Digital I/O Pos. threshold file 2 Power cabling	Motor 2 driving Position threshold 2 ILK PS MD2 ILK Power cabling

TCDQ-CTRL-SERVO-M1

The scope of the fault tree consists of the failure of the PLC to generate the control signal to the DC motor 1 when in servo mode, including signal transmission to the motor 1 power converter. The tree consists of two main branches, see Figure 9. The failure of the electronics is logically combined with the failure of the control signal, which is supervised. The description of the single fault trees with their scope is in Table 11.

PLC-CTRL-SERVO-M1

The scope of the fault tree consists of the failure of the PLC to generate the control signal to motor 1 when in servo mode. The failure can be caused by incorrect set-points as received from the MCS (by FESA application) as well as incorrect time reference from the timing system. This can be in the PLC PID software or in the PLC hardware. The tree consists of five branches at the same level, see Figure 10. The description is in Table 14.

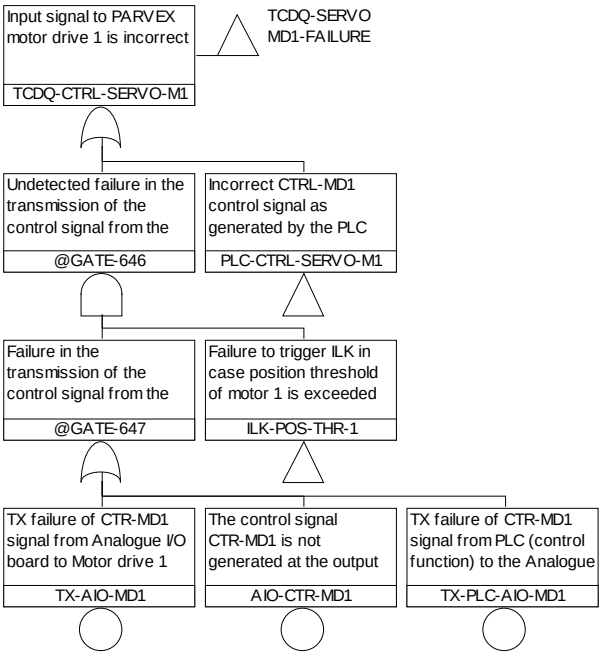

Figure 9: Fault tree of PLC control function of motor 1 in servo mode (doubled triangles are CCF sets)

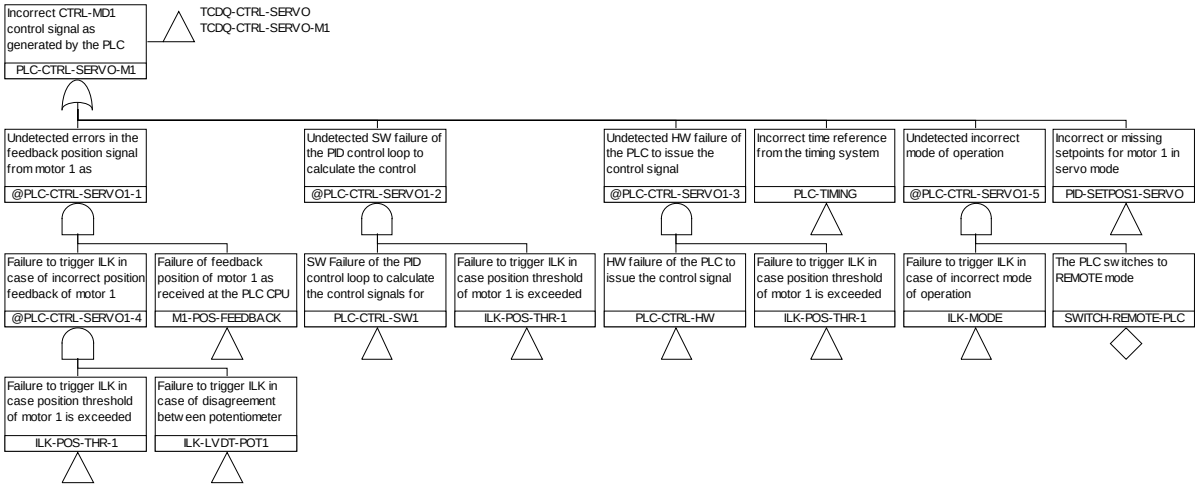

Figure 10: Fault tree of the PLC control function of motor 1 in servo mode

Table 13: Failure events of the TCDQ-CTRL-SERVO-M1 fault tree

PLC-CTRL-SERVO-M1	Models the failure of PLC control function to generate the correct command to DC motor 1	PLC CPU Bus communications ETHERNET Set points table Timing card	Calculation of control signal to motor 1
		PLC CPU Bus communications Analogue I/O Digital I/O ETHERNET Threshold table Potentiometer 1 LVDT	ILK function for position threshold and feedback comparison for motor 1

ILK-POS-THR-1	Models the failure of the PLC interlock function to trigger the ILK to BIC in case the position threshold of motor 1 is exceeded	PLC CPU Bus communications Digital I/O board Threshold table	Position threshold ILK of motor 1
TX-AIO-MD1	Models the failure of the transmission from the Analogue IO board to the motor drive (PARVEX) power converter of motor 1	TX from Analogue I/O output to MD1 input	Control signal motor 1
AIO-CTR-MD1	Models the failure of the analogue IO board to present the control signal of motor 1 at its output	Analogue I/O board output and analogue I/O board	Control signal motor 1
TX-PLC-AIO-MD1	Models the TX failure of control signal of motor 1 from the PLC to the analogue I/O board	PLC Profibus internal communications	Control signal motor 1

Table 14: Failure events of PLC-CTRL-SERVO-M1

Top event ID	**Top event description**	**Systems and components modeled**	**Functions involved**
ILK-POS-THR-1	Models the failure of the PLC interlock function to trigger the ILK to BIC in case the position threshold of motor 1 is exceeded	PLC CPU Bus communications Digital I/O board Threshold table	Position threshold ILK of motor 1
ILK-LVDT-POT1	Models the failure of the PLC interlock function to trigger the ILK to BIC in case the potentiometer and the LVDT disagree	PLC CPU Bus communications Digital I/O board	Position comparison ILK of motor 1
M1-POS-FEEDBACK	Models the failure of the feedback position signal of motor 1 as measured by the potentiometer and received at the PLC CPU	Potentiometer 1 Analogue I/O board Bus communications	Feedback position signal motor 1
PLC-CTRL-SW1	Models the failure of the PID control program (SW) to calculate the correct control signal to motor 1	PLC PID PID parameters	Calculation of control signal motor 1
PLC-CTRL-HW	Models the failure of the PLC CPU to issue the calculated control signal to motor 1	PLC clock PLC rack Bus communications	Output of Control signal motor 1
ILK-POS-THR-1	Models the failure of the PLC interlock function to trigger the ILK to BIC in case the position threshold of motor 1 is exceeded	PLC CPU Bus communications Digital I/O board Threshold table	Position threshold ILK of motor 1

PID-SETPOS1-SERVO	Models incorrect or missing set point of motor 1 as calculated by the MCS in servo mode	FESA application interface ETHERNET board Set points table	PID control motor 1
ILK-MODE	Model the failure to detect the spurious switch from servo to remote mode	PLC CPU Bus communications Digital I/O board	Incorrect operation mode ILK
PLC-TIMING	Models the incorrect time reference as received from the timing system	Start signal from the timing system	Time reference
SWITCH-REMOTE-PLC	Models the spurious change of mode from servo to remote	PLC CPU	Operation mode

TCDQ-CTRL-SERVO-M2

Logic description is identical to the TCDQ-CTRL-SERVO-M1 as well as PLC-CTRL-SERVO2 is identical to PLC-CTRL-SERVO1. Components are of the same kind, with the same failure modes.

TCDQ-SERVO-HOLD

The scope of the fault tree consists of the control chain. Motors and blocker are excluded. The TCDQ may leave the required position for a spurious undetected movement, as it is generated in the PLC, or in the PARVEX motor drives. The tree is built tracking back the signal from the motor drives back to the source of the control signal in the PLC. Failures of signal transmissions are included too. The fault tree is shown in Figure 11, with description in Table 16.

TCDQ-CTRL-SPURIOUS-1

The scope of the fault tree consists of the failure of the TCDQ motor 1 which moves actuated by a spurious control from PLC or a failure of the respective motor drive. The tree consists of four trees and two basic events (spurious control generated in the motor drive), see Figure 12 and description in Table 16. The fault tree PLC-SPURIOUS-M1 is in Figure 13.

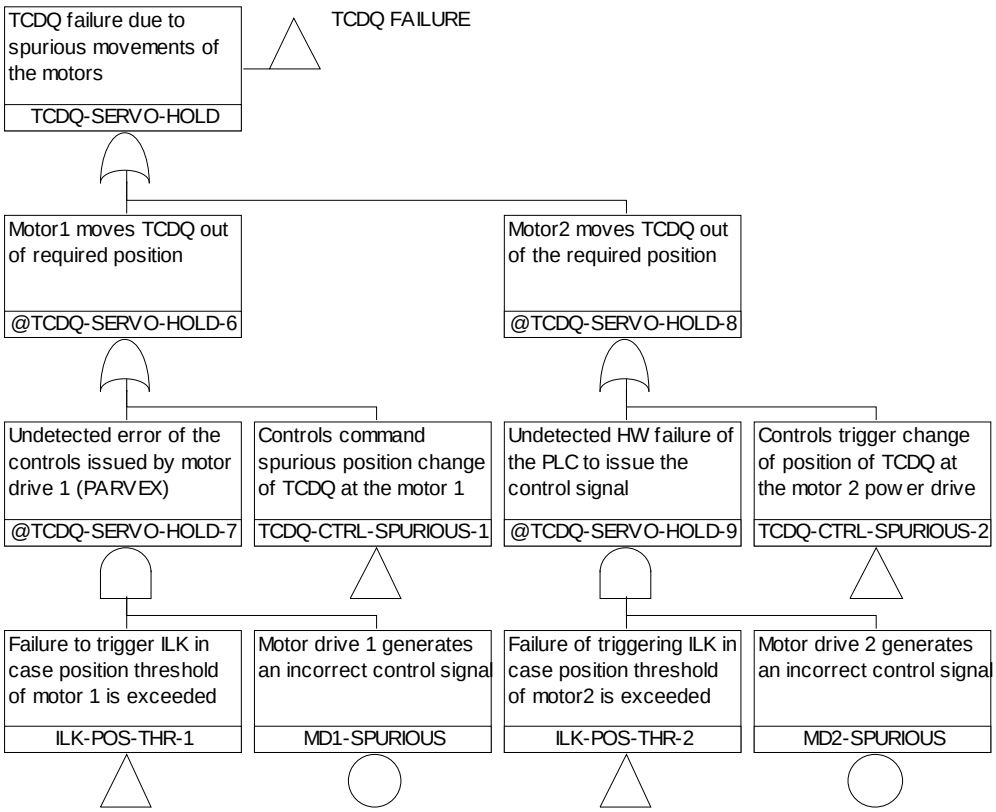

Figure 11: Fault tree of TCDQ failure in servo (automatic) hold position

Table 15: Failure events of TCDQ-SERVO-HOLD

Top event ID	Top event description	Systems and components modeled	Functions involved
TCDQ-CTRL-SPURIOUS-1	Models the failure of PLC control function to generate and transmit a spurious incorrect command to DC motor 1	PLC CPU Bus communications Analogue I/O	Calculation of control signal and transmission to motor 1
		PLC CPU Bus communications Analogue I/O Digital I/O Potentiometer 1 LVDT	ILK function for position threshold and feedback comparison for motor 1
TCDQ-CTRL-SPURIOUS-2	Models the failure of PLC control function to generate and transmit a spurious incorrect command to DC	PLC CPU Bus communications Analogue I/O	Controls calculation and transmission to motor 2

	motor 2	PLC CPU Bus communications Analogue I/O Digital I/O Potentiometer 2 LVDT	ILK function for position threshold and feedback comparison for motor 2
ILK-POS-THR-1	Models the failure of the PLC interlock function to trigger the ILK to BIC in case the position threshold of motor 1 is exceeded	PLC CPU Bus communications Digital I/O board Threshold table	Position threshold ILK of motor 1
ILK-POS-THR-2	Models the failure of the PLC interlock function to trigger the ILK to BIC in case the position threshold of motor 2 is exceeded	PLC CPU Bus communications Digital I/O board Threshold table	Position threshold ILK of motor 1
MD1-SPURIOUS	Models the failure of the motor1 power converter (PARVEX 1) that generates a spurious control to motor 1	MD1 PARVEX electronics	Motor 1 driving
MD2-SPURIOUS	Models the failure of the motor1 power converter (PARVEX 2) that generates a spurious control to motor 2	MD2 PARVEX electronics	Motor 2 driving

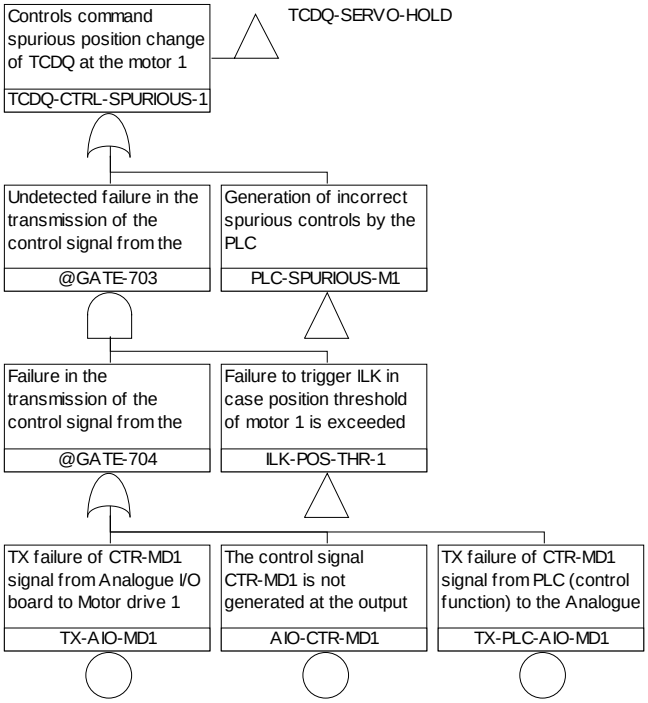

Figure 12: Fault tree of the PLC control function of motor 1

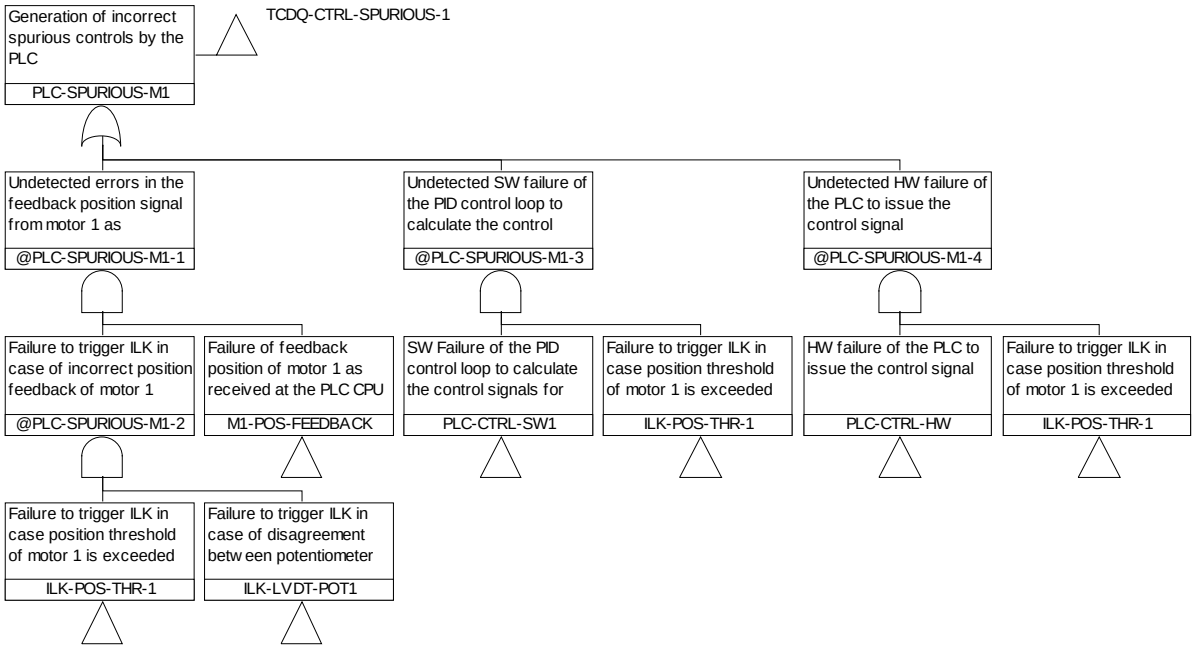

Figure 13: Fault tree of the PLC CPU that generates spurious control to motor1

Table 16: Failure events of the fault tree PLC-CTRL-SPURIOUS-1

Top event ID	Top event description	Systems and components modeled	Functions involved
ILK-POS-THR-1	Models the failure of the PLC interlock function to trigger the ILK to BIC in case the position threshold of motor 1 is exceeded	PLC CPU Bus communications Digital I/O board Threshold table	Position threshold ILK of motor 1
PLC-SPURIOUS-M1	Models the failure of the PLC that generates a spurious control	PLC CPU Bus communications Digital I/O board	Calculation of position controls
TX-AIO-MD1	Failure of control signal from the analogue board to MD1 (failure leading to a spurious)	Analogue communications	Control signal transmission (motor 1)

AIO-CTR-MD1	The control signal is not generated at the output (failure leading to a spurious)	Analogue I/O board	Control signal transmission (motor 1)
TX-PLC-AIO-MD1	Models the failure of the PLC CPU to issue the calculated control signal to analogue I/O board (leading to spurious)	PLC internal board to board communication	Output of control signal motor 1

INAPPROPRIATE-REMOTE

The fault tree models the TCDQ in the inappropriate remote mode when it should be in servo mode. This may happen every time the operator asks for the control and then missed to release it leaving the TCDQ without automatic controls. The fault tree consists of two basic failure events: 1) failure of the operator to release the control into servo mode and 2) the missed detection of incorrect mode of operation. The first failure event is undeveloped.