IEC61508 Overall Safety Requirements and their Allocation Document for PSS0

Review

	Name	Role/Title
Owner	Fan Ye Denis Paulic	PSS Safety Engineer, Isograph Expert, Engineering Safety Consultants Limited, UK Deputy Group Leader for Protection Systems Group, ICS
Reviewer	Stuart Birch Michael Plagge	Senior Engineer - Personnel Safety Systems, ICS Occupational Health & Safety Engineer, ESH
Approver	Annika Nordt	Group Leader for Protection and Safety Systems Group, ICS
Distribution list	Timo Korhonen Ralf Trant Yong Kian Sin	Chief Engineer, Integrated Control System Division Associate Director, ESH&Q Electrical Controls Engineer- Personnel Safety Systems, ICS

TABLE OF CONTENT **PAGE**

Review

LIST OF TABLES

Review

LIST OF FIGURES

Review

1. SCOPE

This report is the IEC61508 Overall Safety Requirements and their Allocation Document for European Spallation Source (ESS) ERIC Personnel Safety System 0 (PSS0). The report provides a Safety Integrity Level (SIL) assessment of the PSS0 Safety Instrumented Functions (SIFs).

The scope of the SIL assessment is limited to the five safety functions identified within the PSS0 Hazard and Risk analysis document ESS-0229506 [1].

2. CONTRIBUTORS

- Dr Fan Ye
- Denis Paulic
- Stuart Birch
- Morteza Mansouri

3. ISSUING ORGANISATION

- Integrated Control System (ICS) Division, European Spallation Source ERIC.

4. INTRODUCTION

4.1. Objectives

This report documents a SIL assessment of the PSS0, conducted in accordance with IEC 61508 [2] and IEC 61511 [3]. The objective of the study was to identify required levels of risk reduction, expressed in terms of SILs, and to verify that the corresponding SIFs meet these targets.

This report documents the:

- Determination of the potential frequency and consequence of agreed hazards;
- Determination of the risk reduction provided by other measures and the resulting risk gap, if any;
- Assignment of SIL requirements for SIFs to any resulting risk gaps in accordance with IEC 61508 [2] and IEC 61511 [3];
- Verification of SIFs against SIL requirements in terms of random hardware reliability and minimum architecture;
- Recommendations for addressing any shortfalls.

4.2. Scope

The scope of this study was limited to the PSS0 Hazards and SIFs identified in the PSS0 Hazard and Risk Analysis document ESS-0229506 [1], supported by the PSS0 Hazard Register [4].

Preview

The study assesses the potential risks to the safety of personnel.

This document covers Safety Lifecycle Phases 4 and 5 from IEC 61508 [2]: Overall Safety requirements and Overall Safety requirements allocation.

The document addresses the requirements of IEC 61511 [3] Phase 2 and Phase 4, as described in the Functional Safety Assessment (FSA) Lifecycle diagram, for hazards that can be directly addressed by the implementation of a SIF.

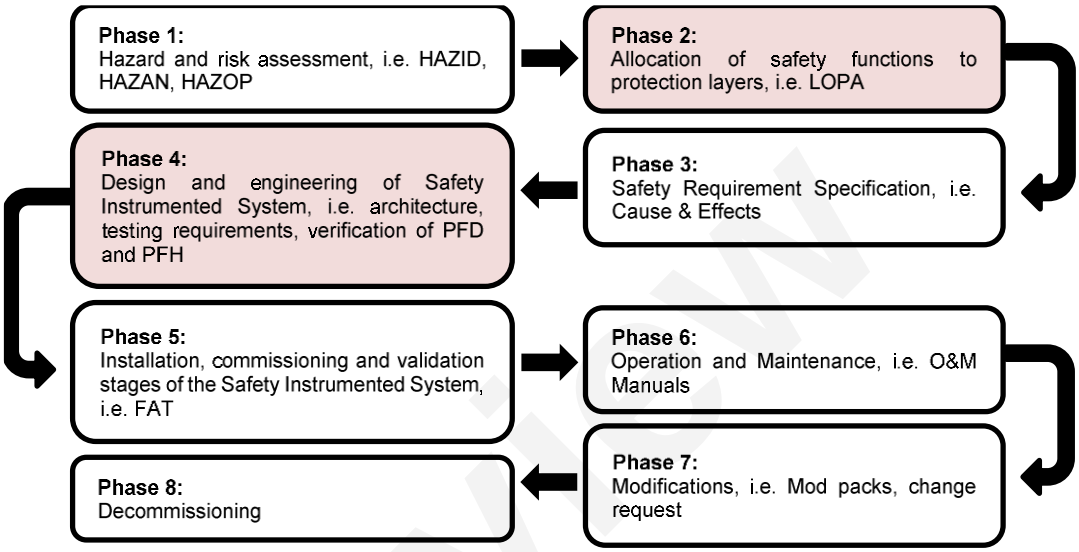


Figure 1: IEC 61511 Functional Safety Assessment Lifecycle Diagram.

4.3. List of SIFs

Table 1 gives a summary of the SIFs and the corresponding Hazard IDs. A more detailed definition of the SIFs can be found at Appendix A (Section 11).

Table 1. List of SIFs

Hazard ID	SIF Tag	SIF Description	Mode of Operation
N/A	SIF01 – HV emergency stop	Upon detecting the emergency stop button being pressed, shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains).	Low Demand
HAZ003 IE01	SIF02 – HV interlock upon intrusion to PSS0 Controlled Area	Upon detecting access gate in open position (1oo2 position switch), shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains).	Low Demand

Review

Hazard ID	SIF Tag	SIF Description	Mode of Operation
HAZ003 IE02	SIF03 – HV interlock – PSS0 Key Exchange	Upon detecting access key is removed (key switch in off position), shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains). Additionally, it also closes an earth relay to remove any residual stored energy from the power supply and its output cable.	High Demand
HAZ003 IE01	SIF04 – Door lock – PSS0 Key Exchange	Upon detecting access key is removed from Slot 2, lock the Access Gate (de-energising 1oo1 solenoid) via Safety PLC (1oo2, blue and red trains).	High Demand
HAZ003 IE01	SIF05 – HV On warning light	HV ON warning light activated when Access Key at Slot 1 in On position.	High Demand

Notes:

- SIF01 was designed to prevent equipment damage in cases of fire or explosion. It is not used for personnel protection and not taken as safeguard for the electric shock hazard. Therefore it has been excluded from any further assessment.
- SIF05 is not a SIF by definition, as it does not put the system in a safe state. However, this function is provided by PSS0. It will be treated as part of administrative control and excluded from any further assessment.

4.4. SIL Determination

4.4.1. General

The assignment of SIL targets was achieved using the Layers of Protection Analysis (LOPA) technique. The LOPA methodology is presented in Section 6.1, and follows the process described in IEC 61511-3 [3] and the American Institute of Chemical Engineers (AIChE) CCPS LOPA 2001 [5]. The LOPA was conducted using ESC's in-house software package: ProSET® v.5.6.1.0.

The LOPA worksheets are presented in Appendix C (Section 13).

4.4.2. Information Used in the LOPA

The following information was provided by ESS PSS team for use in the LOPA study:

- PSS0 Hazard and Risk Analysis document ESS-0229506 [1]
- PSS0 Hazard Register ESS-0229491 [4]

Review

4.5. SIL Verification

The random hardware reliability assessment was performed using isograph FaultTree+ software package, which utilises the Fault Tree Analysis (FTA) method. The hardware reliability assessment methodology is presented in Section 6.2.

An architectural constraints assessment was performed by following Route 1_H of IEC 61508 [2] and the methodology is presented in Section 6.3.

5. ASSUMPTIONS

5.1. Introduction

The following sections detail the data and assumptions applied in the analysis and provide justification for each item.

5.2. SIL Determination Assumptions

This section presents the assumptions and rule set applied in this analysis.

In accordance with the risk matrix presented in the PSS0 Hazard Register [4], the risk target of 1.0E-06 per year has been selected for the LOPA study for analysing the electric shock hazard.

Initiating events frequencies from the PSS0 Hazard and Risk Analysis document [1] were used in the study, as agreed with the ESS PSS team.

Table 2 lists the typical IPLs and associated acceptance criteria applied in the study as guidance, as agreed with ESS PSS team. Justification for these typical data is provided in the ESC Standard LOPA Rule Set [7].

Review

Table 2. IPL Guidance

Device	Typical PFD	Minimum Acceptance Criteria
Alarm (with preventative action in the Control Room)	≥ 0.1	The time between annunciation of the alarm and the hazardous event occurring is ≥ 10 minutes; Operator is trained on alarm response; Operator practices the action periodically; Change on alarm setting is governed by strict Management of Change procedure; Control Room operator error was not the initiating event; The operator has an adequate alarm system; There are written procedures stating the operator action; Alarm falls within safe upper and lower limited and allows timely response from the control room.
Alarm (with preventative action in the field)	≥ 0.1	The time between annunciation of the alarm and the hazardous event occurring is ≥ 30 minutes; Operator is trained on alarm response; Operator practices the action periodically; Change on alarm setting is governed by strict Management of Change procedure; Control Room operator error was not the initiating event; The operator has an adequate alarm system; There are written procedures stating the operator action; Alarm falls within safe upper and lower limited and allows timely response from control room.

Review

Device	Typical PFD	Minimum Acceptance Criteria
BPCS Protective Loop	≥ 0.1	The control loop runs in automatic mode and is subject to access and security control; The loop in question is independent of the initiating or enabling events; The loop is independent of any other device, system or action that is already being credited as an IPL for the same scenario; The control loop (Sensor, Logic and Control valve / contactor) is independent from the SIF for which the SIL target is being set.
SIL1 SIF	$\geq 10^{-2}$ to $< 10^{-1}$	IPL credit can be taken for a SIF if all the following conditions are met: The sensor and final element subsystems are completely independent from the SIF under consideration; The SIF (comprising sensor, logic and final element subsystems) is independent of the initiating event; The SIF must be assigned a SIL target in relation to the credit given for risk reduction and thus must meet ALL requirements (including PFD verification) of the respective SIL. The total of both required SILs is not greater than the capability of the logic solver. (e.g. SIL1 pre-heat trip and a SIL2 furnace pressure trip = total SIL3 to prevent a fan low air flow from causing a combustibles explosion). It is recommended that during LOPA studies, the higher end of the selected SIL PFD range be applied as a placeholder, subject to a random hardware reliability analysis to determine the actual PFD. For example, if credit is taken for a SIL2-rated SIF as an IPL, a PFD of 0.01 should be taken until the actual PFD is determined.
SIL2 SIF	$\geq 10^{-3}$ to $< 10^{-2}$	
SIL3 SIF	$\geq 10^{-4}$ to $< 10^{-3}$	

5.3. SIL Verification Assumptions

The following points summarise the general assumptions used in the analysis. Where possible, specific paragraph references provide the context of the assumption, indicating where it has been applied.

Review

1. If a failure occurs, it is assumed that on average it will occur at the mid-point of the test interval. In other words, the fault will remain undetected for 50% of the test period;

2. The analysis assumes constant failure rates and therefore the effects of early failures are expected to be removed by appropriate processes;

3. Components are not operated beyond their useful life thus ensuring that failures due to wear-out mechanisms do not occur;

4. It is assumed that the SIFs, as defined in Appendix A (Section 11), are sufficient to achieve a safe state;

5. It is assumed that the requirements stated in equipment safety manuals (if applicable) have been adhered to.

6. The proof test interval has been assumed to be once every 2 years;

7. The Proof Test Coverage (PTC) has been assumed to be 100%;

8. The Mean Time to Repair (MTTR) has been assumed to be 8 hours. Spares of key components and maintenance personnel are available onsite.

9. A β factor of 5% for redundant logic solver subsystems and 10% for redundant sensors final element subsystems have been assumed to account for Common Cause Failures (CCFs).

10. Failure rate data in Appendix D (Section 14) have been used for the SIL assessment.

6. METHODLOOGY

6.1. Methodology for SIL Determination

6.1.1. General Concept of Risk Reduction

The purpose of determining the tolerable risk for a specific hazardous event is to state what is deemed reasonable with respect to both the frequency of the hazardous event and its specific consequences.

The tolerable risk will depend on many factors, including the severity of the consequences or injury, the number of people exposed to danger, and the frequency and the duration of the exposure. Important factors will be the perception and views of those exposed to the hazardous event.

Risk reduction is achieved by a combination of all of the available safety protective features, including any associated SIF. The necessary risk reduction to achieve the specified tolerable risk, from a starting point of the risk presented by the Equipment Under Control (EUC), is shown in Figure 2.

Review

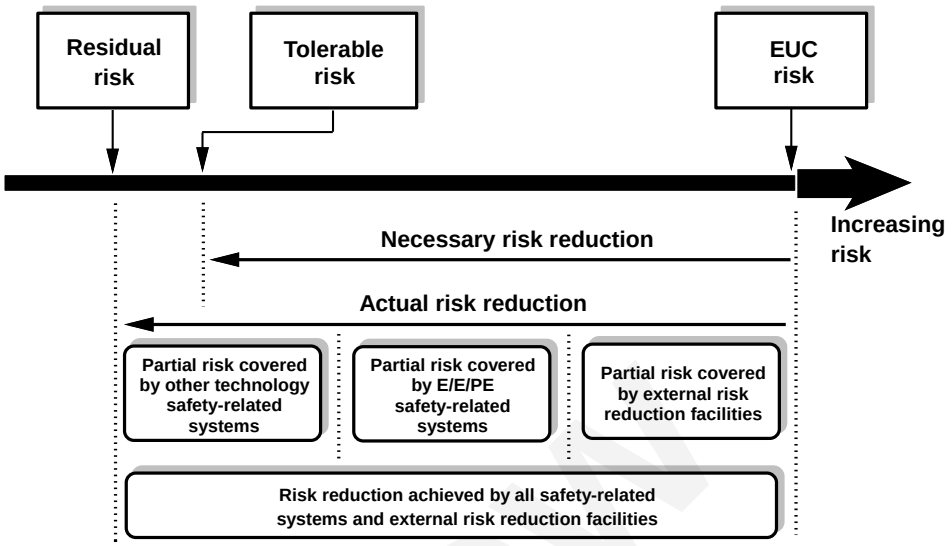


Figure 2. The Concept of Risk Reduction

6.1.2. Risk and Safety Integrity Level

Safety integrity applies to the Electrical / Electronic / Programmable Electronic (E/E/PE) SIF, other technology safety instrumented systems and external risk reduction facilities and is a measure of the likelihood of those systems satisfactorily achieving the necessary risk reduction. Once the tolerable risk has been set, and the necessary risk reduction estimated, the safety integrity requirements for the SIFs can be allocated in terms of PFD or PFH. The PFD and PFH correspond to one of SILs specified in Table 3.

Table 3. SIL Specified PFD

SIL	Low Demand (PFD)	High or Continuous Demand (PFH)
SIL4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
SIL3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
SIL2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
SIL1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
SILa	$\geq 10^{-1}$ to < 1	N/A

"SILa" indicates that although additional mitigation is required, the necessary level of risk reduction is below the SIL1 range and is thus outside the remit of IEC 61508 [2] and IEC 61511 [3]. If, however, an instrumented system is implemented to address a PFD target of greater than 0.1 (i.e. "SILa"), the UK Health and Safety Executive (HSE) requires said function to be subject to the following provisions [6]:

Review

- the persons who have responsibilities for the instrumented system shall be suitably competent;
- clear, precise and unambiguous specification of the safety function;
- independence between control and safety functions wherever reasonably practicable;
- accurate, accessible, controlled and easily understood engineering documentation showing the component parts of the instrumented system and how they are configured. Examples of engineering documentation include loop or circuit diagrams, equipment data sheets and records of parameter settings;
- periodic inspection of the instrumented system, for example visual or more detailed inspection to reveal evidence of deterioration or unexpected modifications;
- periodic maintenance of the instrumented system, for example calibration, cleaning or flushing;
- periodic proof testing of the instrumented system for the purpose of revealing dangerous undetected faults;
- management of change, including control of access to software functions and backing up of software-based systems.

6.1.3. Risk Targets

In UK, HSE guidance on tolerable levels of risk (Reducing Risks, Protecting People [8]) defines the following risk boundaries:

- "*Individual risk of death of one in a million per annum **[1.0E-06/yr]** for both workers and the public corresponds to a very low level of risk and should be used as a guideline for the boundary between the broadly acceptable and tolerable regions*"
- "*Boundary between the 'tolerable' and 'unacceptable' regions for risk entailing fatalities […:] as individual risk of death of one in a thousand **[1.0E-03/yr]** per annum […] for workers*".

Given the inherent inaccuracies in the data applied in SIL determination studies, it was deemed prudent to set the tolerable risk as an order of magnitude lower than the 'tolerable risk boundary'; i.e.1.0E-04/yr. For SIL targeting purposes, this value was typically reduced by a further order of magnitude to account for other, non-process risks of fatality (i.e. slips, trips and falls) to which the hypothetical employee may be exposed.

For the PSS0 SIL study, a more stringent target risk of 1.0E-06 per year was applied as the target for a single employee fatality, as per the PSS0 Hazard Register.

6.1.4. SIL Determination using LOPA

6.1.4.1. General

The assignment of SIL targets was achieved using the LOPA technique, as described in IEC 61511-3 [3] and the AIChE CCPS LOPA 2001 [5].

Review

6.1.4.2. The LOPA Process for Low Demand SIFs

1. Identify hazards (which can be addressed by the implementation of a SIF) using a suitable Process Hazard Analysis tool (e.g. Hazard and Operability Study - HAZOP);

2. Rank the severity of the consequences of the specified hazard. **It is important that existing protection layers are disregarded at this stage.** Compare this with the corresponding risk target in Section 6.1.3;

3. Identify initiating events and estimate their frequency using operating experience where applicable, data sources such as FARADIP [10] and engineering judgement;

4. Identify Conditional Modifiers / Post-Event Mitigation. For example, occupancy, probability of ignition and vulnerability;

5. Identify Independent Protection Layers (IPLs), which prevent the hazardous event from occurring;

6. Determine the likelihood of occurrence (Total Mitigated Event Frequency);

This is calculated by applying equation (1):

$$f^c = \sum_{i=1}^{K} \left[f_i^I \times \left(\prod_{j=1}^{M} PFD_{ij}^{PL} \right) \times \left(\prod_{k=1}^{N} P_{ik}^{CM} \right) \right], \quad (1)$$

where:

f^c is the calculated frequency of consequence *C* summed over all relevant initiating events and with credit taken for all relevant protection layers and conditional modifiers/post-event mitigations: “Total Mitigated Event Frequency”

f_i^I is the frequency of initiating event *i* leading to consequence *C*.

PFD_{ij}^{PL} is the probability of failure on demand of the j[th] protection layer that protects against consequence *C* for initiating event *i.* See “Independent Protection Layers”

P_{ik}^{CM} is the probability that conditional modifier *k* will allow consequence *C* to occur for initiating event *i*. See “Conditional Modifiers”

7. Compare the Target Risk Frequency with the likelihood of occurrence (Total Mitigated Event Frequency) to determine the required PFD for the SIF under consideration. This is calculated by applying equation (2).

$$PFD_{required} = \frac{f^T}{f^c}, \quad (2)$$

Review

where:

f^T is the Target Risk Frequency

8. Determine the SIL requirement of the SIF under consideration by comparing the calculated PFD requirement with Table 3.

6.1.4.3. The LOPA Process for High or Continuous Demand SIFs

1. Identify hazards (which can be addressed by the implementation of a SIF) using a suitable Process Hazard Analysis tool (e.g. Hazard and Operability Study - HAZOP);

2. Rank the severity of the consequences of the specified hazard. **It is important that existing protection layers are disregarded at this stage.** Compare this with the corresponding risk target in Section 6.1.3;

3. Identify Conditional Modifiers / Post-Event Mitigation. For example, occupancy, probability of ignition and vulnerability;

4. Identify Independent Protection Layers (IPLs), which prevent the hazardous event from occurring;

5. Determine the Target Risk Frequency (/hr).

6. This is calculated by applying equation (3):

$$f^T = \left(\prod_{j=1}^{M} PFD_{ij}^{PL}\right) \times \left(\prod_{k=1}^{N} P_{ik}^{CM}\right), \qquad (3)$$

where:

PFD_{ij}^{PL} is the probability of failure on demand of the j[th] protection layer that protects against consequence *C* for initiating event *i.* See "Independent Protection Layers"

P_{ik}^{CM} is the probability that conditional modifier *k* will allow consequence *C* to occur for initiating event *i*.

f^T is the Target Risk Frequency

7. Determine the SIL requirement of the SIF under consideration by comparing the calculated PFH requirement with Table 3.

6.1.4.4. Independent Protection Layers (IPLs)

In order for an IPL to be considered valid (in accordance with IEC 61511-3 [3]), the following criteria must be met:

1. **Effectiveness** – an IPL reduces the identified risk by at least a factor of 10;

Review

2. **Specificity** – an IPL is designed to prevent or mitigate the consequences of one potentially hazardous event. Multiple causes may lead to the same hazardous event, and therefore multiple event scenarios may initiate action by a PL;

3. **Independence** – an IPL is independent of other protection layers if it can be demonstrated that there is no potential for common cause or common mode failure with any other claimed IPL;

4. **Dependability** – an IPL can be counted on to do what it was designed to do by addressing both random failures and systematic failures during its design;

5. **Auditability** – a protection layer is designed to facilitate regular validation of the protective functions.

In order to help achieve and maintain the Auditability criteria (item 5 above), a database of all IPLs applied in this study is presented in Appendix B (Section 12). For the purposes of PFD estimation, it is assumed that all stated IPLs are tested at a proof test interval stated in Section 5.

6.1.5. SIL Determination Results

The LOPA worksheets are presented in Appendix C (Section 13), and the results, together with the established SIL assignment(s), are summarised in Section 13.

6.2. Hardware Reliability Assessment Methodology

6.2.1. Definition of Safety Integrity Level

The hardware reliability of a SIF is expressed in terms of either its Probability of Dangerous Failure on Demand (PFD) or of its Average Frequency of a Dangerous Failure per Hour (PFH[1]), depending on the frequency of demands made upon it.

The frequency of demand ('mode of operation') on the SIF falls into three categories:

- low demand mode (IEC 61508-4: 3.5.16 [2]) – where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or
- high demand mode (IEC 61508-4: 3.5.16 [2]) – where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or
- continuous mode (IEC 61508-4: 3.5.16 [2]) - where the safety function retains the EUC in a safe state as part of normal operation.

[1] The term "probability of dangerous failure per hour" is not used in IEC 61508 **Error! Reference source not found.** but he acronym PFH was retained. When it is used, it means "average frequency of a dangerous failure [h^{-1}]"

Review

6.2.2. Probability of Failure on Demand

For low demand SIFs (refer to section 6.2.1), IEC 61508 [2] requires calculation of the PFD of each complete SIF loop:

$$PFD_{sys} = PFD_s + PFD_L + PFD_{FE}$$ (IEC 61508-6: B.3.2.1 [2]), **(4)**

where:

PFD_{sys} is the probability of failure on demand of a safety function for the electrical/electronic/programmable electronic safety-related system;

PFD_s is the probability of failure on demand for the sensor subsystem;

PFD_L is the probability of failure on demand for the logic subsystem;

PFD_{FE} is the probability of failure on demand for the final element or final element subsystem.

The overall PFD of the complete SIF is compared with its PFD target to determine whether sufficient risk reduction is provided.

6.2.3. Failure Rate, λ

6.2.3.1. General

To calculate the PFD and PFH, it is first necessary to introduce the term ‘failure rate’.

Failure rate is denoted by *λ* and defined as the *number of failures per unit time.*

6.2.3.2. Failure Modes

In order to calculate the PFD of the sensor, logic or final element subsystem using *λ*, its failure modes must first be examined. The number of failures is apportioned into safe and dangerous failure modes, where:

- A **dangerous failure** (IEC 61508-4: 3.6.7 [2]) is defined as a failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:
  - prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or
  - decreases the probability that the safety function operates correctly when required
- A **safe failure** (IEC 61508-4: 3.6.8 [2]) is defined as a failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

Review

- results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or
- increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state

It follows that the total failure rate, λ, is equal to the sum of the safe and dangerous failure rates:

$$\lambda = \lambda_D + \lambda_S , \quad (5)$$

where:

λ_D is the dangerous failure rate per hour and;

λ_S is the safe (or spurious) failure rate per hour.

6.2.3.3. Diagnostic Testing

The dangerous failure rate is further apportioned into dangerous detected and undetected failures, where:

- A **detected** failure (overt) [IEC 61508-4: 3.8 [2]] is defined as a failure, in relation to hardware, detected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation
- An **undetected** failure (covert) [IEC 61508-4: 3.8.9 [2]] is defined as a failure, in relation to hardware, undetected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation

The relationship can therefore be described by:

$$\lambda_D = \lambda_{DD} + \lambda_{DU} , \quad (6)$$

where:

λ_{DD} is the dangerous detected failure rate per hour and;

λ_{DU} is the dangerous undetected failure rate per hour.

6.2.4. PFD and Mean Down Time (MDT)

6.2.4.1. General

The PFD of a single subsystem - for instance, a single detector - is found by multiplying the dangerous failure rate, λ_D (refer to Section 6.2.3.2), by the Mean Down Time (MDT):

$$PFD = \lambda_D MDT, \quad (7)$$

Review

where MDT is the time taken to repair a fault and is, itself, defined as the Mean Time To Repair (MTTR), plus the time taken to detect it. It is assumed that, on average, a fault will occur at the mid-point of the test interval and, thus, the time taken to detect a fault is equal to half the test interval, $T/2$. Therefore:

$$MDT = MTTR + T/2 , \quad \textbf{(8)}$$

6.2.4.2. PFD for Detected Failures

In general, for failures that are detected by the diagnostic tests of a subsystem (refer to Section 6.2.3.3), the test interval (termed as 'diagnostic test interval'), T_d, is typically less than one (1) hour (refer to IEC 61508-6: Annex B [2]) and, thus, the time taken to detect a fault, $T_d/2$, is considered small in comparison with the MTTR. That is:

$MDT_{(Detected)} \approx MTTR$, and thus:

$$PFD_{(Detected)} = \lambda_{DD} MTTR , \quad \textbf{(9)}$$

where MTTR is measured in hours.

6.2.4.3. PFD for Undetected Failures

For undetected failures (refer to Section 6.2.3.3), i.e. failures revealed only by manual proof testing, the MTTR is considered small in comparison with the time taken to detect a fault, i.e. the mid-point of the proof test interval, $T_p/2$; therefore:

$MDT_{(Undetected)} \approx T_p / 2$,

and thus:

$$PFD_{(Undetected)} = \lambda_{DU} T_P / 2 , \quad \textbf{(10)}$$

where T_p is the proof test interval in hours.

6.2.4.4. PFD for Subsystem

The overall PFD of a single subsystem (sensor, logic or final element subsystem), comprises the PFD for undetected faults and the PFD for detected faults:

$$PFD_{subsystem} = PFD_{(Undetected)} + PFD_{(Detected)} . \quad \textbf{(11)}$$

6.2.4.5. PFH for Subsystem

The PFH of a single subsystem - for instance, a single detector - is equivalent to its dangerous undetected failure rate, λ_{DU} (refer to Section 6.2.3.3).

$$PFH_{subsystem} = \lambda_{DU} \quad \textbf{(12)}$$

Review

6.2.5. Voting Configurations

When a subsystem (sensor, logic or final element) consists of several components, such as sensors in a two out of three (2oo3) voting configuration, the combined PFD of the whole subsystem must be calculated. The PFD for subsystems in different configurations are found using the formulae presented in IEC 61508 [2].

The reliability analysis for subsystems in redundant configurations was conducted using the FTA.

6.2.6. Common Cause Failure (CCF)

When assessing the reliability of a subsystem in a redundant configuration, IEC 61508 [2] requires that the effect of CCFs is taken into account. A CCF is defined as: a *failure that is the result of one or more events, causing failures of two or more separate channels in a multiple channel system.*

An example of a CCF would be freezing weather conditions causing identical level transmitters in a 1oo2 voting configuration to fail simultaneously.

CCFs in redundant systems are accounted for using the β model, which assumes a fixed proportion of failures are caused by a common cause. This proportion, termed β, is estimated based on:

- the degree of channel separation;
- design with common cause awareness;
- diagnostic coverage;
- self-test frequency and other factors.

The CCF rate, according to the β model, is calculated as follows:

$$\lambda_{Common\ Cause} = \beta\lambda_{DD} + \beta\lambda_{DU} \quad \textbf{(13)}$$

and, thus, the overall PFD due to dangerous CCFs is given by:

$$PFD_{(Common\ Cause)} = \beta\lambda_{DD}MTTR + \beta\lambda_{DU}T_p / 2 \quad \textbf{(14)}$$

6.3. Architectural Assessment Methodology

6.3.1. Hardware Fault Tolerance (HFT)

In addition to the hardware reliability assessment (refer to Section 6.2), there are also minimum architecture requirements to be met. Each subsystem within a SIF must meet the minimum HFT for the required SIL. That is, the sensor, logic and final element subsystems must all individually meet the overall SIL requirement for the SIF. To determine the level of HFT (or redundancy) required in a SIF using the Route 1_H approach detailed in IEC 61508-2: 7.4.4.2, the Safe Failure Fraction (SFF) must be calculated for each subsystem.

Review

6.3.2. Safe Failure Fraction (SFF)

The SFF is essentially the proportion of random failures in a subsystem that either result in a safe state, or a dangerous state that is revealed by automatic diagnostic tests. SFF is calculated using the following formula:

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_{DD} + \lambda_{DU} + \lambda_S}$$ (IEC 61508-2: C.1.h [2]), **(15)**

where:

λ_{DD} is the dangerous detected failure rate per hour;

λ_{DU} is the dangerous undetected failure rate per hour;

λ_S is the safe (spurious) failure rate per hour.

6.3.3. IEC 61508 Architectural Constraints (Route 1_H)

Table 4 presents the (Route 1_H) minimum HFT for Type A and Type B components respectively. For a component to be considered Type A, all the following criteria must be met:

- Failure modes are well defined and;
- Behaviour under fault conditions is well defined and;
- Failure data is available.

If a component fails to meet any of these criteria, it is considered to be Type B. Type B components typically contain complex microelectronics, commonly found in Programmable Logic Controllers (PLCs) and smart sensors. Simple devices, such as valves and relays, are typically considered to be Type A.

Table 4. HFT for Type A and Type B Components

SFF	Minimum HFT for Type A Component			Minimum HFT for Type B Component		
	SIL for simplex	SIL for m+1	SIL for m+2	SIL for simplex	SIL for m+1	SIL for m+2
	(HFT=0)	(HFT=1)	(HFT=2)	(HFT=0)	(HFT=1)	(HFT=2)
<60%	1	2	3	Not allowed	1	2
60-90%	2	3	4	1	2	3
90-99%	3	4	4	2	3	4
>99%	4	4	4	3	4	4

Review

7. RESULTS

The results of the SIL Assessment are summarised in Table 5 and Table 6.

Table 5. Summary of Results – LOW Demand SIFs

SIF Tag	SIF Description	Hazardous Event (Deviation)	Selected PFD Target	PFD Achieved	Selected SIL Target	Max Allowable SIL (Architectural Constraints)	Result	Status
SIF02 – HV interlock upon intrusion to PSS0 controlled area	Upon detecting access gate in open position (1oo2 position switch), shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains).	High / More Power leading to (Safety) Electric shock	1.0E-3	7.7E-4	SIL 2	SIL 3	Passed	Closed

Review

Table 6. Summary of Results – HIGH Demand SIFs

SIF Tag	SIF Description	Hazardous Event (Deviation)	Selected PFH Target	PFH Achieved	Selected SIL Target	Max Allowable SIL (Architectural Constraints)	Result	Status
SIF03 – HV interlock – PSS0 key exchange	Upon detecting access key is removed (key switch in off position), shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains). Additionally, it also closes an earth relay to remove any residual stored energy from the power supply and its output cable.	High / More Power leading to (Safety) Electric shock	1.1E-7	1.1E-7	SIL 2	SIL 2	Passed	Closed
SIF04 – Door lock – PSS0 key exchange	Upon detecting access key is removed from Slot 2, lock the Access Gate (de-energising 1oo1 solenoid) via Safety PLC (1oo2, blue and red trains).	High / More Power leading to (Safety) Electric shock	1.1E-7	6.0E-8	SIL 2	SIL 2	Passed	Closed

Review

8. CONCLUSIONS AND RECOMMENDATIONS

All assessed SIFs meet their required SIL determined by the LOPA, in terms of achieved PFD or PFH and the architectural constraints assessment.

For the emergency exit to be an effective layer of protection, it is recommended to implement a HV ON warning within the PSS0 controlled area.

9. GLOSSARY

Term	Definition
/hr	per hour
/yr	per year
β	Common cause beta factor, presented as percentage
λ	Failure Rate
λ_{DU}	Dangerous Undetected Failure Rate
λ_{DD}	Dangerous Detected Failure Rate
λ_{D}	Dangerous Failure Rate
λ_{S}	Safe Failure Rate
AIChE	American Institute of Chemical Engineers
BPCS	Basic Process Control System
CCF	Common Cause Failure
CCPS	Center for Chemical Process Safety
E/E/PE	Electrical / Electronic / Programmable Electronic
ERIC	European Research Infrastructure Consortium
ESC	Engineering Safety Consultants
ESS	European Spallation Source
ETA	Event Tree Analysis
EUC	Equipment Under Control
FAT	Factory Acceptance Test
FSA	Functional Safety Assessment
FTA	Fault Tree Analysis
HAZAN	Hazard Analysis
HAZID	Hazard Identification

Review

Term	Definition
HAZOP	Hazard and Operability
HFT	Hardware Fault Tolerance
HSE	Health and Safety Executive
HV	High Voltage
ICS	Integrated Control System
ID	Identifier
IE	Initiating Event
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
LOPA	Layers of Protection Analysis
MDT	Mean Down Time
MRT	Mean Repair Time
MTTR	Mean Time To Repair
oo	out of (voting configuration)
O&M	Operation and Maintenance
PLC	Programmable Logic Controller
PFH	Probability of Failure per Hour
PFD	Probability of Failure on Demand
PSS	Personnel Safety System
PTC	Proof Test Coverage
RBD	Reliability Block Diagram
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
T_p	Proof Test Interval

Review

10. REFERENCES

[1] ESS-0229506: PSS0 Hazard and Risk Analysis Document.

[2] IEC 61508:2010, Functional safety of electrical/ electronic/ programmable electronic safety related systems.

[3] IEC 61511: 2016, Functional safety – Safety instrumented systems for the process industry sector.

[4] ESS-0229491: PSS0 Hazard Register.

[5] The American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS) Layer of Protection Analysis (LOPA) 2001.

[6] UK HSE document: Management of instrumented systems providing safety functions of low / undefined safety integrity (http://www.hse.gov.uk/foi/internalops/hid_circs/technical_general/spc-tech-gen-51.htm#action). Accessed 10th June 2014.

[7] ESC SIL Determination Rule Set: Document Ref. P001_ID090.

[8] HSE document: Reducing risks, protecting people (R2P2), 2001, ISBN 0-7176-2151-0.

[9] Reliability, Maintainability and Risk, DJ Smith, 8th Edition, Butterworth-Heinemann, ISBN 9780080969022.

[10] FARADIP - THREE V9.2, Reliability Data Base, Technis, 26 Orchard Drive, Tonbridge, Kent, TN10 4LG, ISBN 0-951-65623-6.

[11] PSS0 safety device failure rate data file, MS Excel file "RBD data Standards added.xlsx".

Review

11. APPENDIX A – SIF DEFINITIONS

SIF Tag	SIF Description	Sensor Subsystem	Sensor Subsystem Configuration	Logic Subsystem	Logic Subsystem Configuration	Final Element Subsystem	Final Element Subsystem Configuration
SIF01 – HV Emergency Stop	Upon detecting the emergency stop button being pressed, shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains).	PB001	1oo1	LS001, LS002	1oo2	Relay001, C001, Relay002, C002	1oo2
SIF02 – HV interlock upon intrusion to PSS0 controlled area	Upon detecting access gate in open position (1oo2 position switch), shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains).	sw_mag, sw_mech	1oo2	LS001, LS002	1oo2	Relay001, C001, Relay002, C002	1oo2

Review

SIF Tag	SIF Description	Sensor Subsystem	Sensor Subsystem Configuration	Logic Subsystem	Logic Subsystem Configuration	Final Element Subsystem	Final Element Subsystem Configuration
SIF03 – HV interlock – PSS0 key exchange	Upon detecting access key is removed (key switch in off position), shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains). Additionally, it also closes an earth relay to remove any residual stored energy from the power supply and its output cable.	sw_key	1oo1	LS001, LS002	1oo2	Relay001, C001, Relay001, C001	1oo2
SIF04 – Door lock – PSS0 key exchange	Upon detecting access key is removed from Slot 2, lock the Access Gate (de-energising 1oo1 solenoid) via Safety PLC (1oo2, blue and red trains).	sw_key	1oo1	LS001, LS002	1oo2	Solenoid	1oo1
SIF05 – HV ON warning light	HV ON warning light activated when Access Key at Slot 1 in On position.	sw_key	1oo1	LS001, LS002	1oo2	Mains, UPS	1oo2
						WarnLight	1oo1

Review

Notes:

- SIF01 was designed to prevent equipment damage in cases of fire or explosion. It is not used for personnel protection and not taken as safeguard for the electric shock hazard. Therefore it has been excluded from any further assessment.
- SIF05 is not a SIF by definition, as it does not put the system in a safe state. However, this function is provided by PSS0. It will be treated as part of administrative control and excluded from any further assessment.

Review

12. APPENDIX B – IPL REGISTER

Tag	Type	Description	Justification
SIF05 – HV ON warning light	Alarms	HV on warning light and sign	Administrative control
SIF02 – HV interlock upon intrusion to PSS0 controlled area	SIF	Upon detecting access gate opening, isolate power sources to HV via Safety PLC	Placeholder PFD of 1.0E-02 used, pending SIL verification
Formalised Search	Human Factors	Formalised search by personnel. HV is inhibited prior to successful completion of the formalised search.	Personnel conducting the search in a small area, with the aid of the safety system
Emergency Exit	Human Factors	Emergency exit door available, can be opened from inside. Upon door opening, HV will be shutdown (part of AccessGate SIF)	This requires personnel to take action by pushing the emergency exit door
Grounding Rod	Human Factors	Procedure requires personnel to put the grounding rod in place upon entering PSS0 controlled area.	Trained personnel following written procedure

Review

Tag	Type	Description	Justification
SIF03 – HV interlock – PSS0 key exchange	SIF	Key exchange system: Upon detecting access key is removed (key switch in off position), shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains). Additionally, it also closes an earth relay to remove any residual stored energy from the power supply and its output cable.	A placeholder PFD of 1.0E-02 used, pending SIL verification
SIF04 – Door lock – PSS0 key exchange	SIF	SIF - Key exchange system: Upon detecting access key is removed from Slot 2, lock the Access Gate (de-energising 1oo1 solenoid) via Safety PLC (1oo2, blue and red trains).	A placeholder PFD of 1.0E-02 used, pending SIL verification
Procedures	Human Factors	Procedures for formalised search, and grounding rod placement	Trained personnel following written procedure

Review

13. APPENDIX C – SIL ASSESSMENT WORKSHEETS

SIF02 – HV interlock upon intrusion to PSS0 controlled area

This SIF applies to HZ003 IE01 – Personnel attempts access to PSS0 controlled area (when HV is ON).

LOPA Worksheets

HAZARD ID	**HAZ003 IE01**	**SIF Tag**	**SIF02 – HV interlock upon intrusion to PSS0 controlled area**
Drawing Numbers			
SIF Description	Upon detecting access gate in open position (1oo2 position switch), shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains).		
Hazardous Event (Deviation)	High / More Power leading to (Safety) Electric shock		
Mode Of Operation	Low Demand	Nodes	1
Notes			

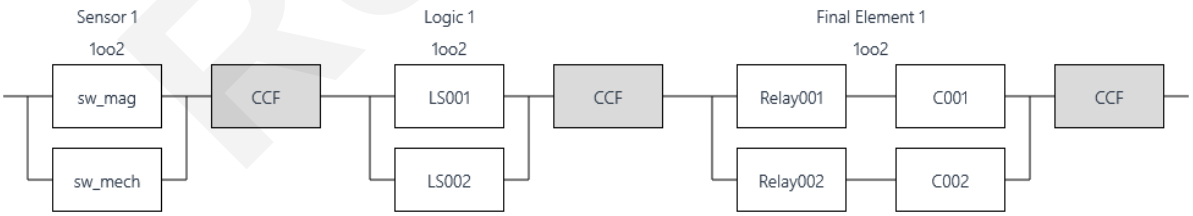
LOPA Summary					
Category	Target Risk Frequency (/yr)	Consequence Description	Total Inter. Event Freq. (/yr)	PFD Target	SIL Target
Safety	1.0E-6	Fatality / Serious Disability / Life Threatening Health Effect	1.0E-3	1.0E-3	SIL 2
				Selected SIL Target	**SIL 2**

Review

Ref.	Initiating Events		IPLs		No Modifiers		Inter. Event Freq. (/yr)
	Description / Justification	Freq. (/yr)	A	B	Type		
1	Personnel attempt to access PSS0 controlled area, whilst HV is On.	1.0E0	Y	Y	Safety		1.0E-3
	Estimated to be 1 per year.						

IPLs / Conditional Modifiers				
Ref.	Type	Tag	Description / Justification	Credit
A	Alarms	SIF05 – HV ON warning light	HV on warning light and sign	1.0E-1
			Administrative control	
B	SIF	SIF04 – Door lock – PSS0 key exchange	Upon detecting access key is removed from Slot 2, lock the Access Gate (de-energising 1oo1 solenoid) via Safety PLC (1oo2, blue and red trains).	1.0E-2
			A placeholder PFD of 1.0E-02 used, pending SIL verification	

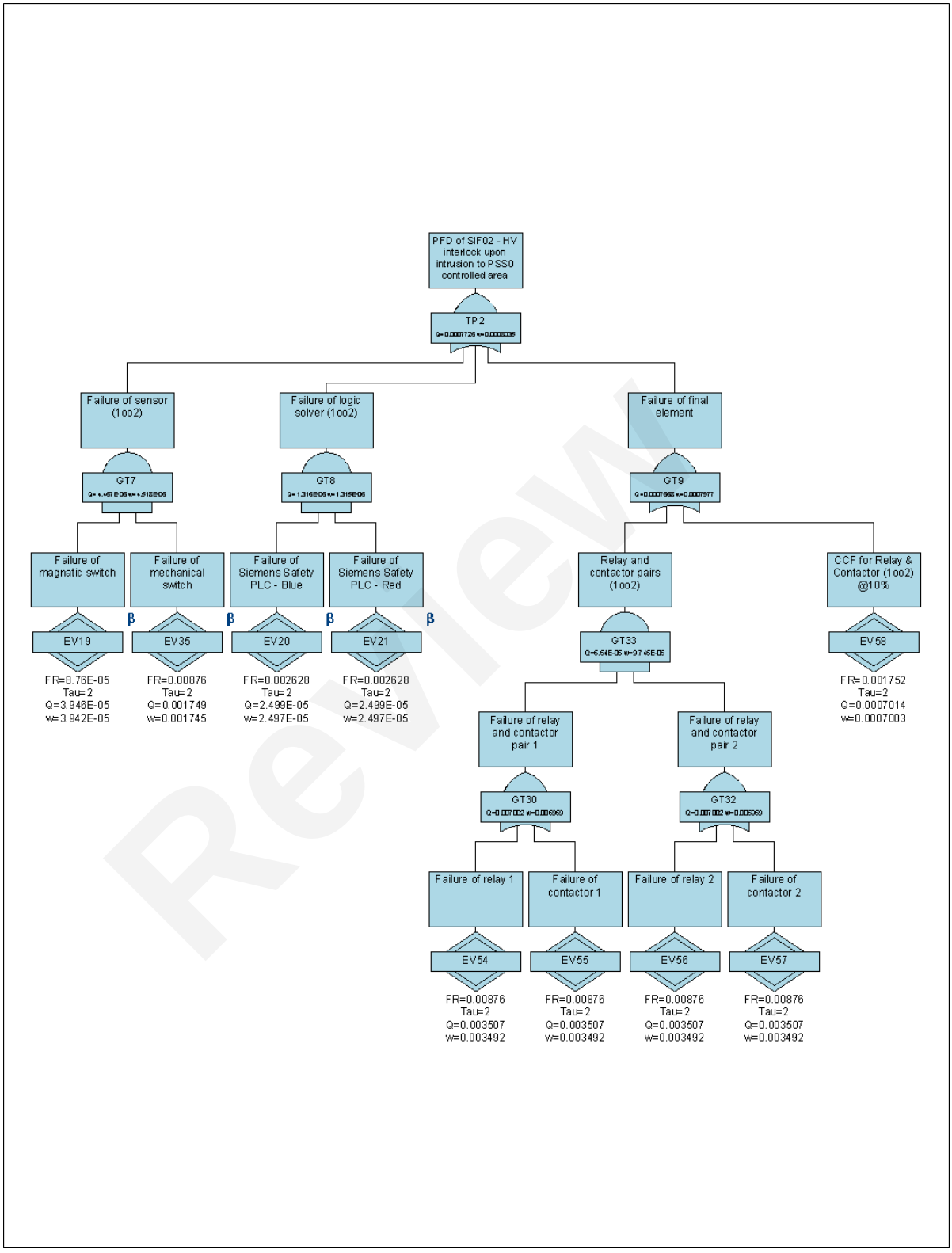
RBD (Reliability Block Diagram)



FTA

The FTA shows the achieved PFD for SIF02 is 7.7E-04. This falls into SIL 3 band.

Review


PFD of SIF02 - HV interlock upon intrusion to PSS0 controlled area
TP2
Failure of sensor (1oo2)
Failure of logic solver (1oo2)
Failure of final element
GT7
GT8
GT9
Failure of magnatic switch
Failure of mechanical switch
Failure of Siemens Safety PLC - Blue
Failure of Siemens Safety PLC - Red
Relay and contactor pairs (1oo2)
CCF for Relay & Contactor (1oo2) @10%
β
β
β
β
EV19
EV35
EV20
EV21
GT33
EV58
FR=8.76E-05
Tau=2
Q=3.946E-05
w=3.942E-05
FR=0.00876
Tau=2
Q=0.001749
w=0.001745
FR=0.002628
Tau=2
Q=2.499E-05
w=2.497E-05
FR=0.002628
Tau=2
Q=2.499E-05
w=2.497E-05
FR=0.001752
Tau=2
Q=0.0007014
w=0.0007003
Failure of relay and contactor pair 1
Failure of relay and contactor pair 2
GT30
GT32
Failure of relay 1
Failure of contactor 1
Failure of relay 2
Failure of contactor 2
EV54
EV55
EV56
EV57
FR=0.00876
Tau=2
Q=0.003507
w=0.003492
FR=0.00876
Tau=2
Q=0.003507
w=0.003492
FR=0.00876
Tau=2
Q=0.003507
w=0.003492
FR=0.00876
Tau=2
Q=0.003507
w=0.003492

Review

SIF03 – HV interlock – PSS0 key exchange

This SIF applies to HZ003 IE02 – HV is turned on by mistake (human error).

LOPA Worksheets

HAZARD ID	HAZ003 IE02	SIF Tag	SIF03 – HV interlock – PSS0 key exchange
Drawing Numbers			
SIF Description	Upon detecting access key is removed (key switch in off position), shutdown HV by removing its power supply (1oo2 relay and contactor) via Safety PLC (1oo2, blue and red trains). Additionally, it also closes an earth relay to remove any residual stored energy from the power supply and its output cable.		
Hazardous Event (Deviation)	High / More Power leading to (Safety) Electric shock		
Mode Of Operation	Continuous	Nodes	1
Notes			

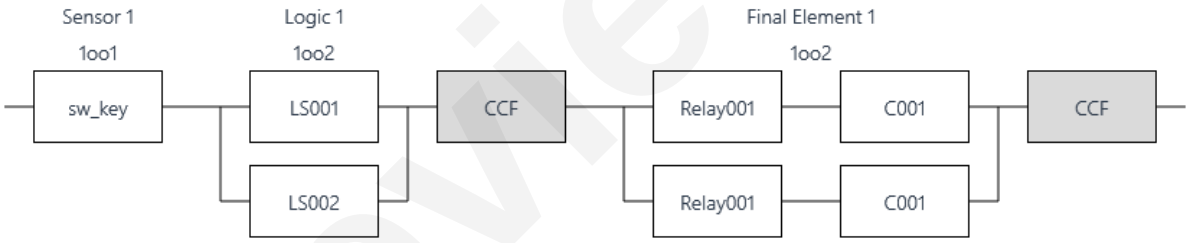
LOPA Summary						
Category	Target Risk Frequency (/hr)	Consequence Description	Total IPL Factors	Total Modifier Factors	PFH Target	SIL Target
Safety	1.1E-10	Fatality / Serious Disability / Life Threatening Health Effect	1.0E-3		1.1E-7	SIL 2
					Selected SIL Target	**SIL 2**

Ref.	Initiating Events		IPLs		No Modifiers	
	Description / Justification	Freq.	A	B	Type	
1	Failure of SIF	N/A	Y	Y	Safety	
	SIF defined as High Demand (>1 demand per year)					

Review

IPLs / Conditional Modifiers				
Ref.	Type	Tag	Description / Justification	Credit
A	Human Factors	Procedures	Procedures for formalised search, and grounding rod placement	1.0E-2
			Trained personnel following written procedure	
B	Human Factors	Emergency Exit	Emergency exit door available, can be opened from inside. Upon door opening, HV will be shutdown (part of SIF for HV interlock upon intrusion to PSS0 controlled area)	1.0E-1
			This requires personnel to take action by pushing the emergency exit door	

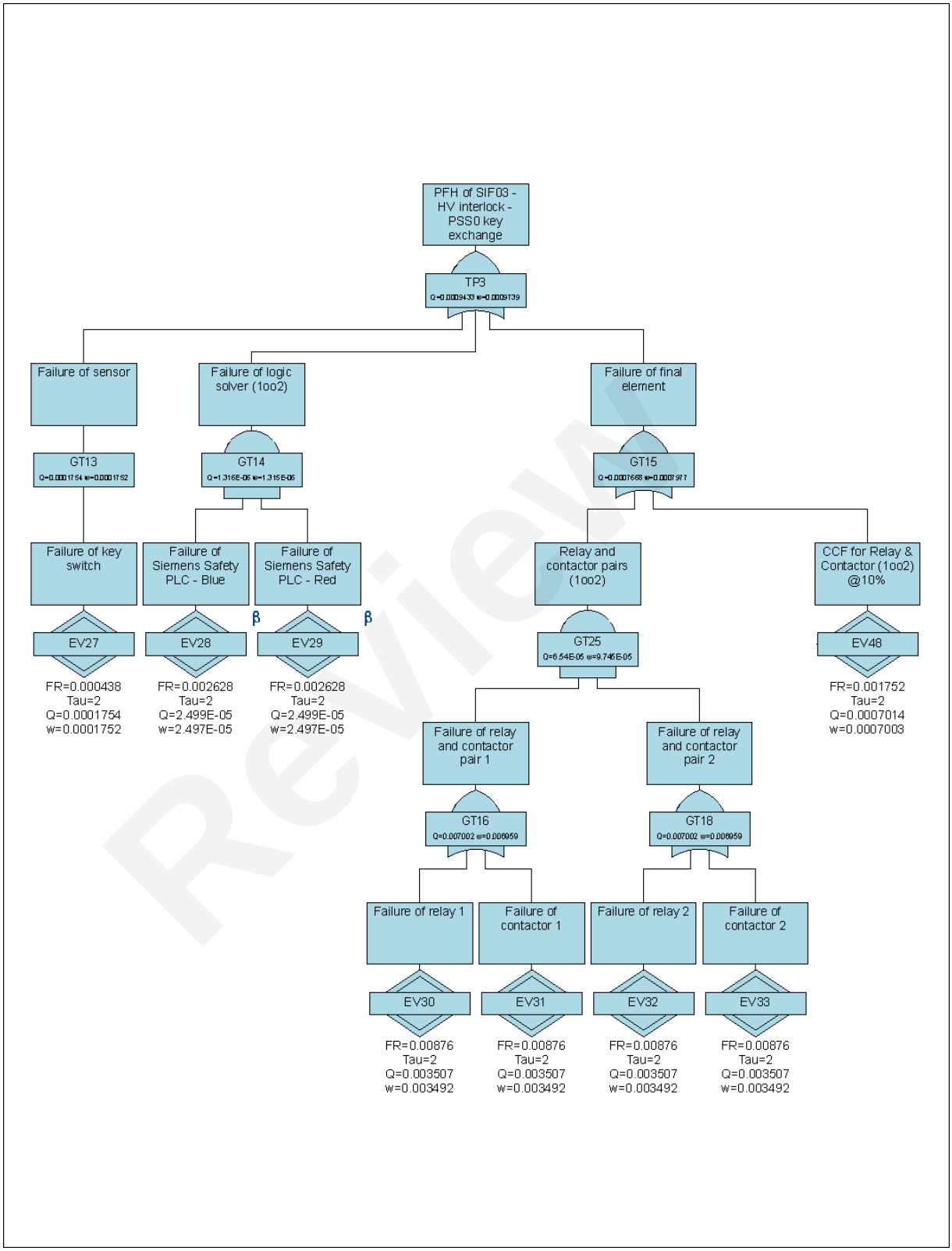
RBD



FTA

The FTA shows the achieved PFH for SIF03 is 9.7E-04 per year, which is 1.1E-07 per hour. This falls into SIL 2 band.

Review


PFH of SIF03 - HV interlock - PSS0 key exchange
TP3
Failure of sensor
Failure of logic solver (1oo2)
Failure of final element
GT13
GT14
GT15
Failure of key switch
Failure of Siemens Safety PLC - Blue
Failure of Siemens Safety PLC - Red
Relay and contactor pairs (1oo2)
CCF for Relay & Contactor (1oo2) @10%
β
β
EV27
EV28
EV29
GT25
EV48
FR=0.000438
Tau=2
Q=0.0001754
w=0.0001752
FR=0.002628
Tau=2
Q=2.499E-05
w=2.497E-05
FR=0.002628
Tau=2
Q=2.499E-05
w=2.497E-05
FR=0.001752
Tau=2
Q=0.0007014
w=0.0007003
Failure of relay and contactor pair 1
Failure of relay and contactor pair 2
GT16
GT18
Failure of relay 1
Failure of contactor 1
Failure of relay 2
Failure of contactor 2
EV30
EV31
EV32
EV33
FR=0.00876
Tau=2
Q=0.003507
w=0.003492
FR=0.00876
Tau=2
Q=0.003507
w=0.003492
FR=0.00876
Tau=2
Q=0.003507
w=0.003492
FR=0.00876
Tau=2
Q=0.003507
w=0.003492

Review

SIF04 – Door lock – PSS0 key exchange

This SIF applies to HZ003 IE01 – Personnel attempts access to PSS0 controlled area (when HV is ON).

LOPA Worksheets

HAZARD ID	**HAZ003 IE01**	**SIF Tag**	**SIF04 – Door lock – PSS0 key exchange**
Drawing Numbers			
SIF Description	Upon detecting access key is removed from Slot 2, lock the Access Gate (de-energising 1oo1 solenoid) via Safety PLC (1oo2, blue and red trains).		
Hazardous Event (Deviation)	High / More Power leading to (Safety) Electric shock		
Mode Of Operation	Continuous	Nodes	1
Notes			

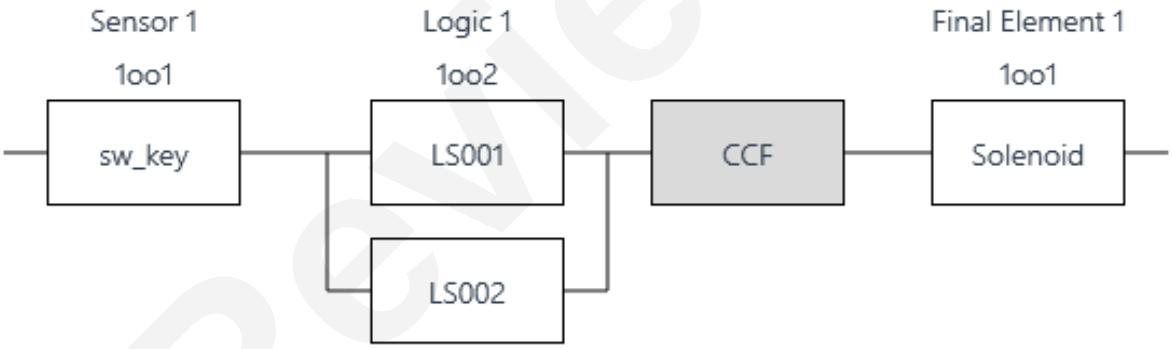
LOPA Summary						
Category	Target Risk Frequency (/hr)	Consequence Description	Total IPL Factors	Total Modifier Factors	PFH Target	SIL Target
Safety	1.1E-10	Fatality / Serious Disability / Life Threatening Health Effect	1.0E-3		1.1E-7	SIL 2
					Selected SIL Target	**SIL 2**

Ref.	Initiating Events		IPLs		No Modifiers	
	Description / Justification	Freq.	A	B	Type	
1	Failure of SIF	N/A	Y	Y	Safety	
	SIF defined as High Demand (>1 demand per year)					

Review

IPLs / Conditional Modifiers				
Ref.	Type	Tag	Description / Justification	Credit
A	Alarms	WarnSign	HV on warning light and sign	1.0E-1
			Administrative control	
B	SIF	SIF02 – HV interlock upon intrusion to PSS0 controlled area	Upon detecting access gate opening, isolate power sources to HV via Safety PLC	1.0E-2
			Placeholder PFD of 1.0E-02 used, pending SIL verification	

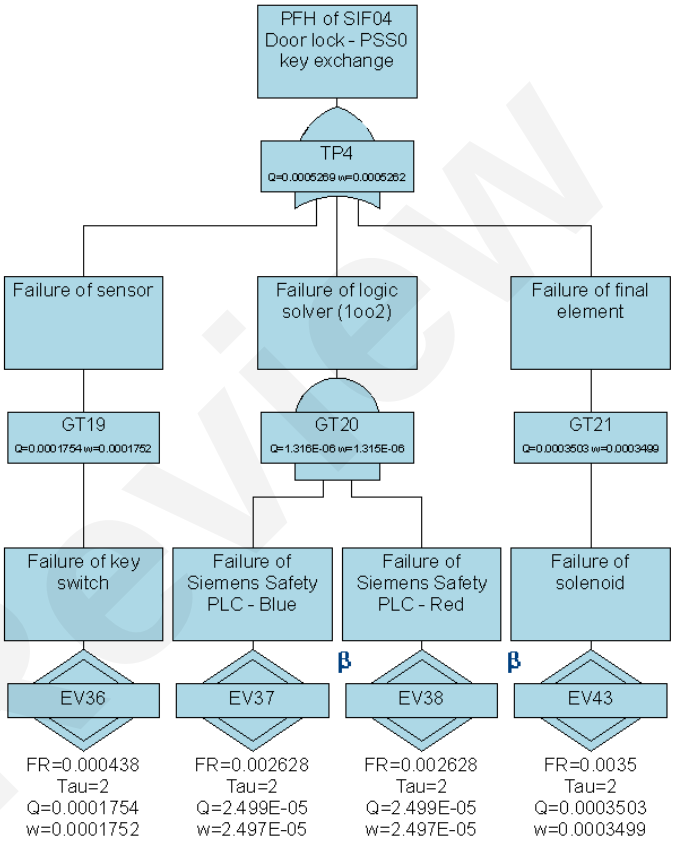
RBD



FTA

The FTA shows the achieved PFH for SIF04 is 5.3E-04 per year, which is 6.0E-08 per hour. This falls into SIL 3 band.

Review


PFH of SIF04 Door lock - PSS0 key exchange
TP4
Q=0.0005269 w=0.0005262
Failure of sensor
Failure of logic solver (1oo2)
Failure of final element
GT19
Q=0.0001754 w=0.0001752
GT20
Q=1.316E-06 w=1.315E-06
GT21
Q=0.0003503 w=0.0003499
Failure of key switch
Failure of Siemens Safety PLC - Blue
Failure of Siemens Safety PLC - Red
Failure of solenoid
β
β
EV36
EV37
EV38
EV43
FR=0.000438
Tau=2
Q=0.0001754
w=0.0001752
FR=0.002628
Tau=2
Q=2.499E-05
w=2.497E-05
FR=0.002628
Tau=2
Q=2.499E-05
w=2.497E-05
FR=0.0035
Tau=2
Q=0.0003503
w=0.0003499

Review

14. APPENDIX D – FAILURE RATE DATA

Device Tag	Manufacturer	Device	Proof Testing Interval (Months)	Proof Testing Coverage (%)	MRT (Hours)	Dangerous Failure Mode	λDD (/hr)	λDU (/hr)	λS (/hr)	SFF (%)	Data Source	Type
C001, C002	Siemens	SIRIUS Contactor 3RT1015-1BB41 **[NOTE 1]**	24	100	8	Fail to open	0	4.0E-7	6.0E-7	60	Siemens IC 10 catalog "Industrial Controls" issue 2015 chapter 16 pages 16-17, October 2015.	A
LS001, LS002	Siemens	SIMATIC S7-1500F + Digital Input (F-DI 8x24VDC HF) + Digital Output (F-DQ 4xDC 24V/2A)	24	100	8	Fail to initiate action	0	3.0E-9	3.0E-7	99	Siemens device manual, December 2014	B
Relay001, Relay002	Siemens	SIRIUS Contactor 3RT1015-1BB41 **[NOTE 1]**	24	100	8	Fail to open	0	4.0E-7	6.0E-7	60	Siemens IC 10 catalog "Industrial Controls" issue 2015 chapter 16 pages 16-17, October 2015.	A

Review

Device Tag	Manufacturer	Device	Proof Testing Interval (Months)	Proof Testing Coverage (%)	MRT (Hours)	Dangerous Failure Mode	λDD (/hr)	λDU (/hr)	λS (/hr)	SFF (%)	Data Source	Type
Solenoid	Siemens	Solenoid door lock, de-energise to lock; Faradip data 0.4fpmh, 10% fail to release, 10% leak, 80% not energise	24	100	8	Failure to release	0	4.0E-8	3.6E-7	90	FARADIP-THREE v9.2	A
sw_key	Fortress Interlocks	mGard S and SE key switch	24	100	8	Fail in open position	0	2.0E-8	3.0E-8	60	Manufacturers mGard Datasheet: SE key switch February 2015; S key switch October 2015	A
sw_mag	Siemens	3SE6604-2BA, SIGUARD Magnetically operated switching element	24	100	8	Fail in closed position	0	5.0E-9	5.0E-9	50	Overview of Safety-Related Parameters from Siemens Components in Accordance with ISO 13849-1 and IEC 62061, May 2013	A

Review

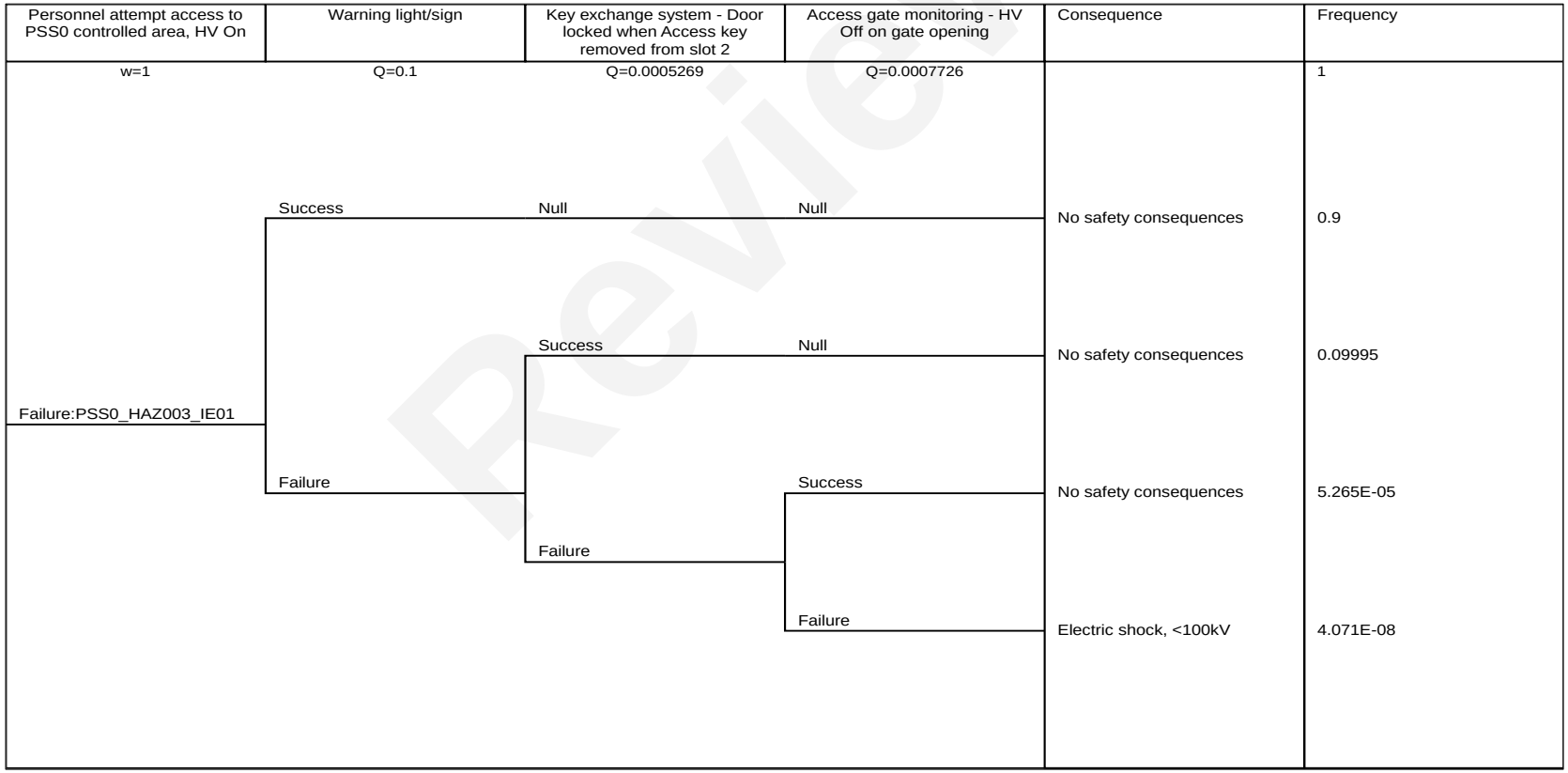
Device Tag	Manufacturer	Device	Proof Testing Interval (Months)	Proof Testing Coverage (%)	MRT (Hours)	Dangerous Failure Mode	λDD (/hr)	λDU (/hr)	λS (/hr)	SFF (%)	Data Source	Type
sw_mech	Siemens	3SE5312-0SH11, safety position switch with solenoid interlocking **[NOTE 1]**	24	100	8	Fail in open position	0	2.0E-7	8.0E-7	80	Siemens IC 10 catelog "Industrial Controls" issue 2015 Chapter 16 pages 16-17, October 2015	A

Note 1: Devices of the same type but with different part number from those listed in [11] are treated as standard device, i.e. not specifically designed for safety application, and non-safety related devices have been assigned a failure rate one order of magnitude higher than the corresponding safety-related devices in [11].

Review

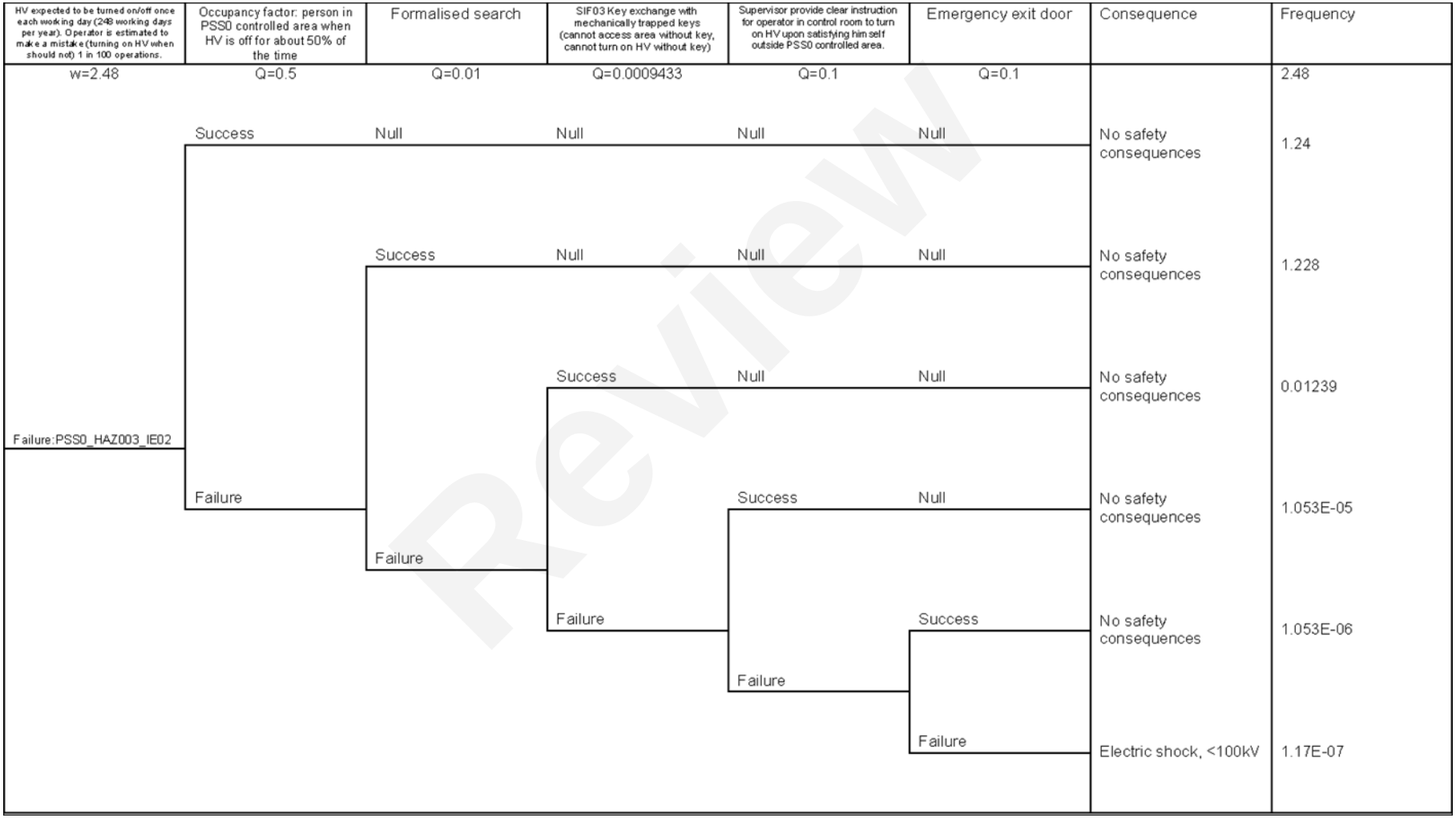
15. APPENDIX E – ETA

HAZ003 IE01



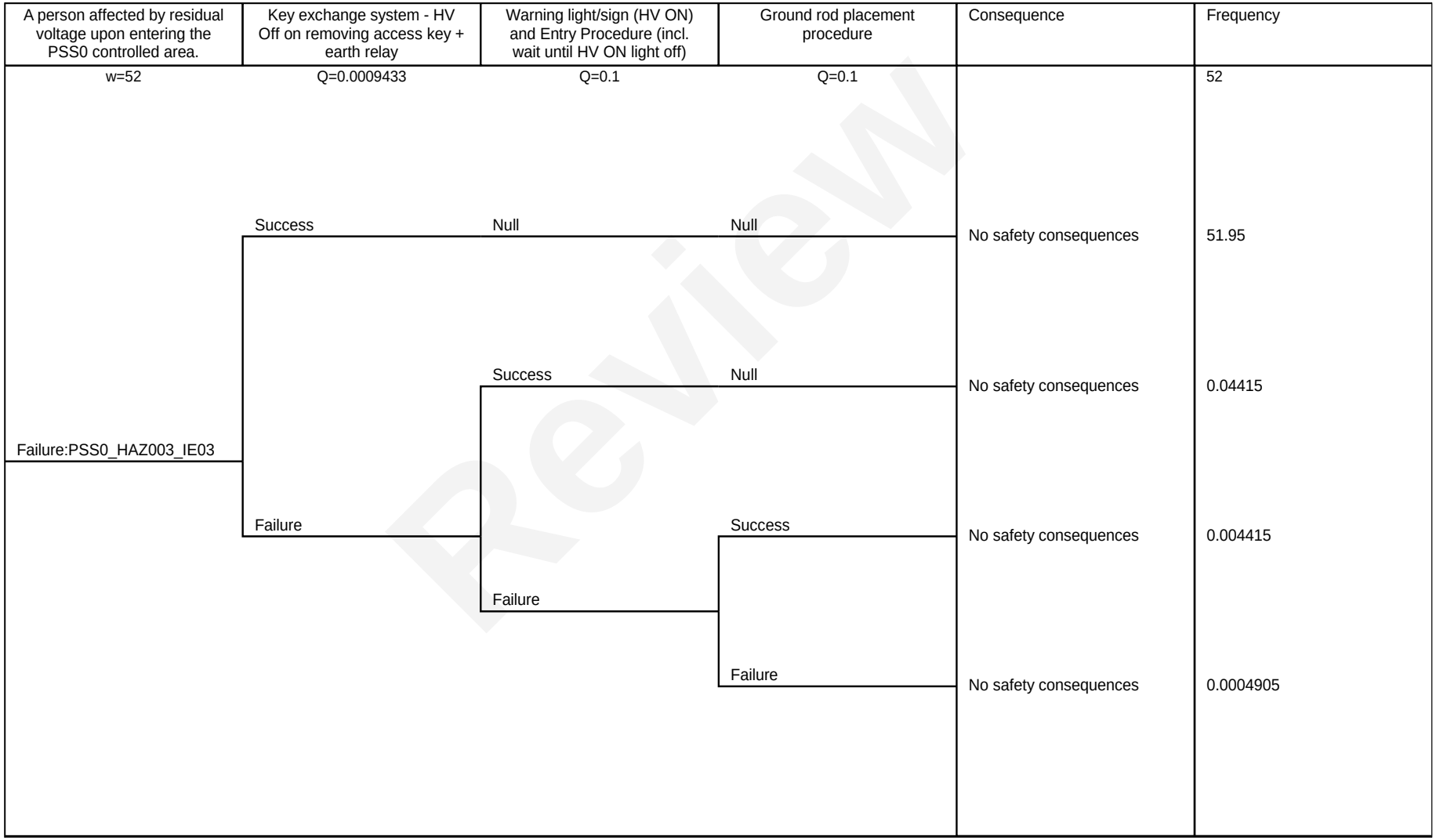
Review

HAZ003 IE02



Review

HAZ003 IE03



Review

Note: upon HV shutdown, the capacitors and cable will discharge any residual energy in 250ms through the 10 MOhm resistors. Gaining access to the PSS0 controlled area using the key exchange system following HV shutdown would take longer than 250ms. As a result, the initiating event is not considered credible for any safety consequences.

Review

DOCUMENT REVISION HISTORY

Revision	Reason for and description of change	Author	Date
1	First issue	Fan Ye	2018-02-05

Review