|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Safety Integrity Level (SIL) Assessment Report for PSS0 |
|  |
|  |

|  | Name | **Role/Title** |
| --- | --- | --- |
| **Authors** | Fan Ye | PSS Safety Engineer, Isograph Expert, Engineering Safety Consultants Limited, UK |
| **Owner** | Stuart Birch | Senior Engineer - Personnel Safety Systems, ICS |
| **Reviewer** | Denis Paulic  Morteza Mansouri  Edgar Sargsyan  Michael Plagge | Deputy Group Leader for Protection and Safety Systems Group, ICS  Lead integrator Engineer for safety critical systems, ICS  Section Leader for Front End & Magnets Section, AD  Occupational Health & Safety Engineer |
| **Approver** | Peter Jacobsson  Annika Nordt | Head of Safety, health and environment division, ESH  Group Leader for Protection and Safety Systems Group, ICS |

|  |  |
| --- | --- |
| Table of content | Page |

1. INTRODUCTION 4

1.1. Objectives 4

1.2. Scope 4

1.3. List of SIFs 5

1.4. SIL Determination 6

1.4.1. General 6

1.4.2. Information Used in the LOPA 6

1.5. SIL Verification 6

2. ASSUMPTIONS 7

2.1. Introduction 7

2.2. SIL Determination Assumptions 7

2.3. SIL Verification Assumptions 7

3. results 9

4. CONCLUSIONS AND RECOMMENDATIONS 11

5. Glossary 11

6. references 12

Appendix a – sif definitions 14

Appendix B – IPL Register 16

Appendix C – SIL ASSESSMENT WORKSHEETS 18

Appendix d – failure rate data 27

appendix e – eTA 30

Document Revision history 32

list of tables

Table 1. List of SIFs 5

Table 2. Summary of Results – LOW Demand SIFs 9

Table 3. Summary of Results – HIGH Demand SIFs 10

list of Figures

Figure 1: IEC 61511 Functional Safety Lifecycle Diagram. 5

# INTRODUCTION

This document is the Safety Integrity Level (SIL) Assessment Report for European Spallation Source (ESS) ERIC Personnel Safety System 0 (PSS0) Safety Instrumented Functions (SIFs). The SIL Assessment covers both SIL Determination and SIL Verification for the PSS0 SIFs.

## Objectives

This report documents a SIL assessment of the PSS0 SIFs, conducted in accordance with IEC 61511 [1]. 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 61511 [1];
* Verification of SIFs against SIL requirements in terms of random hardware reliability and minimum architecture;
* Recommendations for addressing any shortfalls.

## Scope

The scope of this study was limited to the PSS0 SIFs identified in the PSS0 Overall Safety Requirements [2], supported by the Hazard and risk assessment of Ion Source and Low Energy Beam Transport (LEBT) [3] and the Hazard register [4].

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

The document addresses the requirements of [1] Phase 2 and Phase 4, as described in the IEC 61511 Functional Safety Lifecycle diagram, for hazards that can be directly addressed by the implementation of a SIF.



Figure 1: IEC 61511 Functional Safety Lifecycle Diagram.

## 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 (Appendix a – sif definitions).

Table 1. List of SIFs

| Hazard ID | SIF Tag | SIF Description | Mode of Operation |
| --- | --- | --- | --- |
| N/A\* | PSS0\_SIF01 – ISrc HV OFF button | Upon detecting the HV pushbutton being pressed, switch off HV by removing its supplied power (1oo2 relay and contactor) via a safety PLC (1oo2, blue and red trains). | Low Demand |
| Hazard\_003 IE\_01 | PSS0\_SIF02 – HV interlock upon intrusion to PSS0 Controlled Area | Upon detecting access door in open position (1oo2 position switch), switch off HV by removing its supplied power (1oo2 relay and contactor) via a safety PLC (1oo2, blue and red trains). | Low Demand |
| Hazard\_003 IE\_02 | PSS0\_SIF03 – HV interlock – PSS0 Key Exchange | Upon detecting access key is removed from the key exchange switch, switch off HV by removing its supplied power (1oo2 relay and contactor) via a 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 |
| Hazard\_003 IE\_01 | PSS0\_SIF04 – Door lock – PSS0 Key Exchange | Upon detecting access key in key exchange switch (position ON), lock the Access Door (de-energising 1oo1 solenoid) via a safety PLC (1oo1, red train only). | High Demand |

**\*Note:**

* PSS0\_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.

## SIL Determination

### General

The assignment of SIL targets was achieved using the Layers of Protection Analysis (LOPA) technique. The LOPA methodology is presented in the PSS0 Safety Planning document [5], and follows the process described in [1] and the American Institute of Chemical Engineers (AIChE) CCPS LOPA 2001 [6]. The LOPA was conducted using ESC’s in-house software package: ProSET® v.5.6.1.0 [7].

The LOPA worksheets are presented in Appendix C – SIL ASSESSMENT WORKSHEETS.

### Information Used in the LOPA

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

* PSS0 Concept of Operation [8]
* PSS0 Overall safety requirements [2]
* Hazard and risk assessment of ion source and LEBT [3]
* PSS0 Hazard register [4]

## SIL Verification

The 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 the PSS0 Safety Planning document [5].

The architectural constraints assessment was performed by following Route 1H of IEC 61508 [9], which would meet the requirements of IEC 61511 [1]. The methodology is presented in the PSS0 Safety Planning document [5].

Event Tree Analysis (ETA) has been used to confirm that the achieved hazardous events frequencies meet the ESS risk targets.

# ASSUMPTIONS

## Introduction

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

## SIL Determination Assumptions

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

In accordance with the risk matrix presented in [10], the risk target of 1.0E-06 per year has been selected for the LOPA study for analysing the electric shock hazard (leading to a single fatality).

Initiating events frequencies from [2] were used in the study, as agreed with the ESS PSS team.

Independent Protection Layers (IPLs) and associated acceptance criteria applied in the study has been agreed with the ESS PSS team. Justification for the risk reduction credits taken of typical IPLs is provided in the ESC Standard LOPA Rule Set [11].

## 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.

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 – sif definitions, 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 **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 (Appendix d – failure rate data) have been used for the SIL assessment.

# results

The results of the SIL Assessment are summarised in Table 2 (low demand SIFs) and Table 3 (high demand SIFs).

Table 2. 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 |
| PSS0\_SIF02 – HV interlock upon intrusion to PSS0 controlled area | Upon detecting access door in open position (1oo2 position switch), switch off HV by removing its supplied power (1oo2 relay and contactor) via a safety PLC (1oo2, blue and red trains). | Electric shock | 1.0E-3 | 5.6E-4 | SIL 2 | SIL 2 | Passed | Closed |

Table 3. 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 |
| PSS0\_SIF03 – HV interlock – PSS0 key exchange | Upon detecting access key is removed from the key exchange switch, switch off HV by removing its supplied power (1oo2 relay and contactor) via a 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. | Electric shock | 1.1E-7 | 8.6E-8 | SIL 2 | SIL 2 | Passed | Closed |
| PSS0\_SIF04 – Door lock – PSS0 key exchange | Upon detecting access key in key exchange switch (position ON), lock the Access Door (de-energising 1oo1 solenoid) via a safety PLC (1oo1, red train only). | Electric shock | 1.1E-7 | 1.1E-7 | SIL 2 | SIL 2 | Passed | Closed |

# CONCLUSIONS AND RECOMMENDATIONS

All assessed SIFs meet their required SIL as 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.

# Glossary

| Term | Definition |
| --- | --- |
| /hr | per hour |
| /yr | per year |
| ** | Common cause beta factor, presented as percentage |
| λ | Failure Rate |
| λDU | Dangerous Undetected Failure Rate |
| λDD | Dangerous Detected Failure Rate |
| λD | Dangerous Failure Rate |
| λS | Safe Failure Rate |
| AIChE | American Institute of Chemical Engineers |
| 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 |
| FAT | Factory Acceptance Test |
| FTA | Fault Tree Analysis |
| HAZAN | Hazard Analysis |
| HAZID | Hazard Identification |
| HAZOP | Hazard and Operability |
| HV | High Voltage |
| ConOps | Concept of Operations |
| ICS | Integrated Control System |
| ID | Identifier |
| IE | Initiating Event |
| IEC | International Electrotechnical Commission |
| IPL | Independent Protection Layer |
| ISrc | Ion Source |
| LEBT | Low Energy Beam Transport |
| LOPA | Layers of Protection Analysis |
| MTTR | Mean Time To Repair |
| oo | out of (voting configuration) |
| O&M | Operation and Maintenance |
| PLC | Programmable Logic Controller |
| PFH | Average frequency of a dangerous 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 |

# references

1. IEC 61511: 2016, Functional safety – Safety instrumented systems for the process industry sector.
2. ESS-0414418: PSS0 Overall Safety Requirements.
3. ESS-0118213: Hazards and risk assessment of the Ion Source and LEBT.
4. ESS-0229491: PSS0 Hazard Register.
5. ESS-0405652: PSS0 Safety Planning Document.
6. The American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS) Layer of Protection Analysis (LOPA) 2001.
7. ESC ProSET (the complete Process Safety Evaluation Toolset) software package, <http://www.esc.uk.net/proset-software/>.
8. ESS-0134492: PSS0 Concept of Operations (ConOps).
9. IEC 61508:2010, Functional safety of electrical/ electronic/ programmable electronic safety related systems.
10. ESS-0379511: Risk matrix for conventional safety risks.
11. ESC SIL Determination Rule Set: Document Ref. P001\_ID090.
12. FARADIP - THREE V9.2, Reliability Data Base, Technis, 26 Orchard Drive, Tonbridge, Kent, TN10 4LG, ISBN 0-951-65623-6.
13. PSS0 safety device failure rate data file, MS Excel file "RBD data Standards added.xlsx".

# 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 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| PSS0\_SIF01 – ISrc HV OFF button | Upon detecting the HV OFF pushbutton being pressed, switch off HV by removing its supplied power (1oo2 relay and contactor) via a safety PLC (1oo2, blue and red trains). | Pushbutton | 1oo1 | Safety PLC + Relay, Safety PLC + Relay | 1oo2 | Contactor, Contactor | 1oo2 |
| PSS0\_SIF02 – HV interlock upon intrusion to PSS0 controlled area | Upon detecting access door in open position (1oo2 position switch), switch off HV by removing its supplied power (1oo2 relay and contactor) via a safety PLC (1oo2, blue and red trains). | Magnetic Switch, Mechanical Switch | 1oo2 | Safety PLC + Relay, Safety PLC + Relay | 1oo2 | Contactor, Contactor | 1oo2 |
| PSS0\_SIF03 – HV interlock – PSS0 key exchange | Upon detecting access key is removed from the key exchange switch, switch off HV by removing its supplied power (1oo2 relay and contactor) via a 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. | Key Switch | 1oo1 | Safety PLC + Relay, Safety PLC + Relay | 1oo2 | Contactor, Contactor | 1oo2 |
| PSS0\_SIF04 – Door lock – PSS0 key exchange | Upon detecting access key in key exchange switch (position ON), lock the Access Door (de-energising 1oo1 solenoid) via a safety PLC (1oo1, red train only). | Key Switch | 1oo1 | Safety PLC | 1oo1 | Solenoid | 1oo1 |

**Notes:**

* PSS0\_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.

# Appendix B – IPL Register

| Tag | Type | Description | Justification |
| --- | --- | --- | --- |
| HV ON warning light | Alarms | HV on warning light and sign. | Administrative control. PFD of 0.1 taken. |
| PSS0\_SIF02 – HV interlock upon intrusion to PSS0 controlled area | SIF | Upon detecting access door opening, isolate power sources to HV via Safety PLC. | Placeholder PFD of 1.0E-02 used, pending SIL verification. SIL verification (see FTA for PSS0\_SIF02) confirms PFD of 5.6E-04. |
| 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. PFD of 0.01 taken. |
| Emergency Exit | Human Factors | Emergency exit door available, can be opened from inside. Upon door opening, HV will be switched off (part of PSS0\_SIF02) | This requires personnel to take action by pushing the emergency exit door. PFD of 0.1 taken. |
| PSS0\_SIF03 – HV interlock – PSS0 key exchange | SIF | Key exchange system – access key interlock:  Upon detecting access key is removed from the key exchange switch, switch off HV by removing its supplied power (1oo2 relay and contactor) via a 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. SIL verification (see FTA for PSS0\_SIF03) confirms PFD of 7.4E-04. |
| PSS0\_SIF04 – Door lock – PSS0 key exchange | SIF | Key exchange system – door lock:  Upon detecting access key in key exchange switch (position ON), lock the Access Door (de-energising 1oo1 solenoid) via a safety PLC (1oo1, red train only). | A placeholder PFD of 1.0E-02 used, pending SIL verification. SIL verification (see FTA for PSS0\_SIF04) confirms PFD of 9.9E-04. |

# Appendix C – SIL ASSESSMENT WORKSHEETS

**PSS0\_SIF02 – HV interlock upon intrusion to PSS0 controlled area**

This SIF applies to Hazard\_003 IE\_01 – Personnel attempts access to PSS0 controlled area (when HV is ON).

**LOPA Worksheets**

| HAZARD ID | Hazard\_003 IE\_01 | | SIF Tag | PSS0\_SIF02 – HV interlock upon intrusion to PSS0 controlled area | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Drawing Numbers |  | | | | | | |
| SIF Description | Upon detecting access door in open position (1oo2 position switch), switch off HV by removing its supplied power (1oo2 relay and contactor) via a safety PLC (1oo2, blue and red trains).  Additionally, the SIF also closes an earth relay (i.e. the HV grounding relay) to remove any residual stored energy from the power supply and its output cable in case of intrusion, with some delay after the main contactors are open. | | | | | | |
| Hazardous Event (Deviation) | 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 | Single fatality | | | 1.0E-3 | 1.0E-3 | SIL 2 |
| Selected SIL Target | | | | | | | **SIL 2** |

| 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 | HV ON warning light | HV on warning light and sign | 1.0E-1 |
| Administrative control |
| B | SIF | PSS0\_SIF04 – Door lock – PSS0 key exchange | Upon detecting access key in key exchange switch (position ON), lock the Access Door (de-energising 1oo1 solenoid) via a safety PLC (1oo1, red train only). | 1.0E-2 |
| A placeholder PFD of 1.0E-02 used, pending SIL verification |

**RBD**

The figure below presents the Reliability Block Diagram (RBD) for PSS0\_SIF02. The configuration achieves SIL 2 in terms of architectural constraints.



**FTA**

The FTA shows the achieved PFD for PSS0\_SIF02 is 5.6E-04. This falls into SIL 3 band.



**PSS0\_SIF03 – HV interlock – PSS0 key exchange**

This SIF applies to Hazard\_003 IE\_02 – HV is turned on by mistake (human error).

**LOPA Worksheets**

| HAZARD ID | Hazard\_003 IE\_02 | | SIF Tag | PSS0\_SIF03 – HV interlock – PSS0 key exchange | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Drawing Numbers |  | | | | | | | |
| SIF Description | Upon detecting access key is removed from the key exchange switch, switch off HV by removing its supplied power (1oo2 relay and contactor) via a 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) | 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 | Single fatality | | | 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) |  |

| 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 switched off (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**

The figure below presents the RBD for PSS0\_SIF03. The configuration achieves SIL 2 in terms of architectural constraints.



**FTA**

The FTA shows the achieved PFH for PSS0\_SIF03 is 7.5E-04 per year, which is 8.6E-08 per hour. This falls into SIL 3 band.



**PSS0\_SIF04 – Door lock – PSS0 key exchange**

This SIF applies to Hazard\_003 IE\_01 – Personnel attempts access to PSS0 controlled area (when HV is ON).

**LOPA Worksheets**

| HAZARD ID | Hazard\_003 IE\_01 | | SIF Tag | PSS0\_SIF04 – Door lock – PSS0 key exchange | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Drawing Numbers |  | | | | | | | |
| SIF Description | Upon detecting access key in key exchange switch (position ON), lock the Access Door (de-energising 1oo1 solenoid) via a safety PLC (1oo1, red train only). | | | | | | | |
| Hazardous Event (Deviation) | 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 | Single fatality | | | 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) |  |

| 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 | PSS0\_SIF02 – HV interlock upon intrusion to PSS0 controlled area | Upon detecting access door opening, isolate power sources to HV via safety PLC | 1.0E-2 |
| Placeholder PFD of 1.0E-02 used, pending SIL verification |

**RBD**

The figure below presents the RBD for PSS0\_SIF04. The configuration achieves SIL 2 in terms of architectural constraints.



**FTA**

The FTA shows the achieved PFH for PSS0\_SIF04 is 9.9E-04 per year, which is 1.1E-07 per hour. This falls into SIL 2 band.



# Appendix d – failure rate data

| Device Tag | Manufacturer | Device | Proof Testing Interval (Months) | Proof Testing Coverage (%) | MTTR (Hours) | Dangerous Failure Mode | λDD (/hr) | λDU (/hr) | λS (/hr) | SFF (%) | Data Source | Type |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Relay, Contactor | 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 |
| Safety PLC | 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 |
| 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 | 9.0E-8 | 5.1E-7 | 85 | FARADIP-THREE v9.2 [12] | A |
| Key Switch | Fortress Interlocks | mGard S and SE key switch | 24 | 100 | 24 | 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 |
| Magnetic Switch | 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 |
| Mechanical Switch | 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 [13] 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 [13].

# appendix e – eTA

**Hazard\_003 IE\_01**



**Hazard\_003 IE\_02**



Document Revision history

| Revision | Reason for and description of change | Author | Date |
| --- | --- | --- | --- |
| 1 | First issue | Fan Ye | 2018-02-05 |
| 2 | Updated to align with the PSS0 Hazard and Risk Analysis Document ESS-0229506. | Fan Ye | 2018-05-21 |
| 3 | Updated to move SIL Assessment methodologies to PSS0 Safety Planning Document. Updated PSS0\_SIF04, and addressed internal comments. | Fan Ye | 2018-10-10 |
| 4 | Updated to align with the new PSS0 safety document structure (hazard analysis by asset owner, overall safety requirements, hazard register, and so on). | Fan Ye | 2018-11-05 |
|  |  |  |  |