|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Safety Requirements Specification Document for PSS0 |
|  |
|  |

|  | Name | **Role/Title** |
| --- | --- | --- |
| **Authors**  | Fan Ye  | PSS Safety Engineer, Isograph Expert, Engineering Safety Consultants Limited, UK |
| **Owner** | Stuart Birch | Senior Engineer – Protection Systems Group. Personnel Safety Systems, ICS  |
| **Reviewer** | Denis PaulicMorteza Mansouri Riccard Andersson  | Deputy Group Leader for Protection Systems Group, ICSLead integrator- Protection Systems Group Engineer for safety critical systems, ICS Technical Project Coordinator Engineer for Protection Systems Group, ICS  |
| **Approver** | Annika Nordt | Group Leader for Protection Systems Group, ICS  |

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

1. INTRODUCTION 3

1.1. General 3

1.2. Scope 3

1.3. Document structure 4

2. Safety Requirement Specification 5

2.1. SRS for the SIS Logic Solver 5

2.2. SRS for the SIFs 6

2.2.1. PSS0\_SIF01 – PSS0 ISrc HV OFF 6

2.2.2. PSS0\_SIF02 – HV interlock upon intrusion to PSS0 controlled area 7

2.2.3. PSS0\_SIF03 – HV interlock – PSS0 Key Exchange 8

2.2.4. PSS0\_SIF04 – Door lock – PSS0 Key Exchange 9

3. Glossary 11

4. references 12

Document Revision history 12

list of tables

Table 1. List of SIFs 4

list of Figures

Figure 1: IEC 61511 Functional Safety Lifecycle Diagram. 3

# INTRODUCTION

This document is the Safety Requirement Specification (SRS) for European Spallation Source (ESS) ERIC Personnel Safety System 0 (PSS0). The report provides an SRS for the PSS0 Safety Instrumented Functions (SIFs).

## General

This document defines the safety requirements of each SIF that form the Safety Instrumented System (SIS) associated with the ESS ERIC PSS0.

It includes specifications of both the functional and safety integrity requirements based on documents provided by ESS PSS Team Safety Integrity Level (SIL) assessment carried out in [1].

## Scope

This document covers Safety Lifecycle Phase 3 of IEC 61511 [2].

Figure 1 presents an overview of the IEC 61511 [2] Functional Safety lifecycle. The highlighted block in this diagram indicates the phase applicable to this document.



Figure 1: IEC 61511 Functional Safety Lifecycle Diagram.

The scope of this study covers the four SIFs proposed to address the hazards identified by the Hazard and risk assessment of Ion Source and Low Energy Beam Transport (LEBT) [3] supported by the PSS0 Overall Safety Requirements [4], the PSS0 Hazard Register [5], and the PSS0 SIL Assessment Report [1] produced by ESS PSS Team, which incorporates the SIL Determination and Verification analysis. Table 1 gives a summary of the SIFs and the corresponding Hazard IDs.

Table 1. List of SIFs

| Hazard ID | SIF Tag | SIF Description | Mode of Operation |
| --- | --- | --- | --- |
| N/A\* | PSS0\_SIF01 – ISrc HV OFF | Upon detecting the ISrc HV OFF button being pressed, shutdown of 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), shutdown of 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 (key switch in off position), shutdown of 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 (1oo2, blue and red trains). | High Demand |

**\*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.

## Document structure

The Safety Requirement Specification (SRS) is split into two sections:

1. The general requirements for the SIS;
2. The requirements of each individual SIF.

The SRS for the SIS logic solver is presented in Section 2.1 whilst the SRS for each identified SIF is presented in Section 2.2.

# Safety Requirement Specification

## SRS for the SIS Logic Solver

|  |
| --- |
| SIS Details |
| Operator Interfaces | There is an operator touch screen for each of the 2 trains. |
| SIS BPCS Interfaces | The SIS sends a signal to BPCS PLC (hard-wired from red train DO module) to shut down the HV with a delay of 500 millisecond.The SIS also sends the “PSS OK” status signal to BPCS PLC (hard-wired from red train DO module) to inform operators in the local control room about the SIS status. There is no communication from BPCS to SIS. |
| **Process Details** |
| Normal Plant Operation | The normal operating modes in which the SIS will be expected to operate are:* HV ON
* Access
* Search
 |
| Abnormal Plant Operation | The abnormal operating modes in which the SIS will be expected to operate are: * Alarm
 |
| **SIL Data** |
| SIS SIL Target | SIL 2 |
| SIS Target Proof Test Interval (Months) | 24 |
| SIS Mean Repair Time (Hours) | 8 |
| **Trip Actions** |
| Specific Requirements Related To SIS Start Up / Restart | After restart / start-up SIS shall always be in Access Mode and restart shall be confirmed by acknowledging from operator touch screen.  |
| **Application Program** |
| Limitations and constraints of the hardware and embedded software | None. Siemens proven-in-use devices and safety library will be used. Any constraints and limitations listed in Siemens safety-PLC safety manual shall be observed. |
| Real time performance, sequencing and time delays | Delay of SIS shutdown of HV to allow BPCS shutdown:500 millisecond. |
| Diagnostics, Self-Monitoring and Monitoring of other devices | Built-in diagnostics by Siemens PLC. |
| Functions to enable Periodic Testing | Periodic Testing shall be conducted when the system is not used during normal operation. |
| Requirements for process variable validation and handling of bad process variables | Addressed in Verification and Validation Plan document [6]. |
| Requirements for communication interfaces | No requirements on communication interfaces. |
| Additional Logic Functions | None identified. |
| Application Program Documentation | To be provided at a later stage and documented in the PSS0 Software Planning Document [7]. |
| **Security Requirements** |
| Security Requirements for the SIS, including counter measures to be implemented in the Logic Solver and Application Program | Security analyses will not be conducted for PSS0, but security measures will be taken into account.PSS0 will be a stand-alone system and can only be accessed locally from a PSS laptop. |
| **Environmental Conditions** |
| Design requirements | Will be addressed in PSS0 Hardware Design Requirements Specification [8].  |

## SRS for the SIFs

### PSS0\_SIF01 – PSS0 ISrc HV OFF

|  |
| --- |
| SIF Details |
| SIF Tag | PSS0\_SIF01 |
| Drawing Number | N/A |
| Hazardous Event | This was not designed for safety but rather for emergency situations such as fire or explosion within the PSS0 controlled area, to protect equipment from damage. |
| SIF Description | Upon detecting ISrc HV OFF button being pressed, shutdown of HV by removing its supplied power (1oo2 relay and contactor) via a safety PLC (1oo2, blue and red trains). |
| Sources of Demand | Emergency situations with human intervention |
| Demand Rate on SIF | <1 per year, estimated |
| Trip Points | ISrc HV OFF button being pressed |
| Success Criteria | HV is OFF due to power supply being isolated |
| Functional Relationship (Between Input and Output) | HV OFF upon pressing the ISrc HV OFF button. |
| **Common Cause Failures** |
| Electrical Power Loss | System is safe as HV will be off upon power loss. |
| Compressed Air Loss | N/A |
| Hydraulic Pressure Loss | N/A |
| **Process Details** |
| Safe State Definition | HV is powered off. |
| Hazards from Concurrent Safe States | None identified. |
| Process Safety Time | N/A |
| Requirement to Survive a Major Accident | None identified. Loss of power due to major accidents will put system in safe state. |
| **SIL Data** |
| Mode of Operation | Low Demand |
| SIL | Target | N/A | Achieved | N/A |
| PFD / PFH | Target | N/A | Achieved | N/A |
| Spurious Trip Rate (/hr) | Target | No availability requirement for PSS0 | Achieved | N/A |
| Target Proof Test Interval (Months) | Sensor Subsystem | Final Element Subsystem |
| ISrc HV OFF button | 24 | Contactor | 24 |
|  |  | Contactor | 24 |
| Mean Repair Time (hours) | Sensor Subsystem | Final Element Subsystem |
| ISrc HV OFF button | 8 | Contactor | 8 |
|  |  | Contactor | 8 |
| SIF Response Time Achieved | N/A |
| **Trip Actions** |
| Manual Shutdown Requirements | The process can be shut down via BPCS. |
| Energise / De-Energise To Trip | De-energise to trip |
| Requirements for Resetting after Shutdown | The HV power supply needs to be manually reset following a shutdown. |
| Overrides / Inhibits / Bypasses (including control measures for when these are in use) | There are no overrides / inhibits / bypasses for this SIF. |
| Dangerous Combinations of Output States | None identified. |
| Actions to Achieve / Maintain Safe State | Ensure power supply to HV is isolated. |
| Action on Valve Discrepancy | N/A |
| **Desired Responses to SIF Failure Modes Properties** |
| Sensor Failures | Fail to detect ISrc HV OFF button being pressed |
| Logic Solver Failures | Fail to initiate action |
| Final Element Failures | Fail to open relay / contactor |
| **Maintenance Issues** |
| Maintenance Considerations | Maintenance shall be conducted as per device manuals and project operation and maintenance procedures. |

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

|  |
| --- |
| SIF Details |
| SIF Tag | PSS0\_SIF02 |
| Drawing Number | N/A |
| Hazardous Event | Hazard\_003 IE\_01, Electric shock from attempted access to PSS0 controlled area while HV is ON. |
| SIF Description | Upon detecting access door in open position (1oo2 position switch), shutdown of HV by removing its supplied power (1oo2 relay and contactor) via a safety PLC (1oo2, blue and red trains). |
| Sources of Demand | Human error, attempting to access PSS0 controlled area whilst HV is on. |
| Demand Rate on SIF | Estimated to be once per year. |
| Trip Points | Access door opening (detected by position switches) |
| Success Criteria | HV is OFF due to power supply being isolated |
| Functional Relationship (Between Input and Output) | HV OFF upon opening of access door. |
| **Common Cause Failures** |
| Electrical Power Loss | System is safe as HV will be off upon power loss. |
| Compressed Air Loss | N/A |
| Hydraulic Pressure Loss | N/A |
| **Process Details** |
| Safe State Definition | HV is powered off. |
| Hazards from Concurrent Safe States | None identified. |
| Process Safety Time | About 4 seconds. |
| Requirement to Survive a Major Accident | None identified. Loss of power due to major accidents will put system in safe state. |
| **SIL Data** |
| Mode of Operation | Low Demand |
| SIL | Target | SIL 2 | Achieved | SIL 2 |
| PFD / PFH | Target | 1.0E-03 | Achieved | 5.6E-04 |
| Spurious Trip Rate (/hr) | Target | No availability requirement for PSS0 | Achieved | N/A |
| Target Proof Test Interval (Months) | Sensor Subsystem | Final Element Subsystem |
| Magnetic switch | 24 | Contactor | 24 |
| Mechanical switch | 24 | Contactor | 24 |
| Mean Repair Time (hours) | Sensor Subsystem | Final Element Subsystem |
| Magnetic switch | 8 | Contactor | 8 |
| Mechanical switch | 8 | Contactor | 8 |
| SIF Response Time Achieved | < 1 second (total time from detection to system in safe state, including PLC scanning time, and delay to allow BPCS to achieve normal shutdown) |
| **Trip Actions** |
| Manual Shutdown Requirements | ISrc HV OFF is provided via a pushbutton. The process can also be shut down via BPCS. |
| Energise / De-Energise To Trip | De-energise to trip |
| Requirements for Resetting after Shutdown | The HV power supply needs to be manually reset following a shutdown. |
| Overrides / Inhibits / Bypasses (including control measures for when these are in use) | There are no overrides / inhibits / bypasses for this SIF. |
| Dangerous Combinations of Output States | None identified. |
| Actions to Achieve / Maintain Safe State | Ensure power supply to HV is isolated. |
| Action on Valve Discrepancy | N/A |
| **Desired Responses to SIF Failure Modes Properties** |
| Sensor Failures | Fail to detect door opening |
| Logic Solver Failures | Fail to initiate action |
| Final Element Failures | Fail to open relay / contactor |
| **Maintenance Issues** |
| Maintenance Considerations | Maintenance shall be conducted as per device manuals and project operation and maintenance procedures. |

### PSS0\_SIF03 – HV interlock – PSS0 Key Exchange

|  |
| --- |
| SIF Details |
| SIF Tag | PSS0\_SIF03 |
| Drawing Number | N/A |
| Hazardous Event | Hazard\_003 IE\_02, Electric shock when HV is turned on by mistake. |
| SIF Description | Upon detecting access key is removed (key switch in off position), shutdown of 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. |
| Sources of Demand | Human error, HV is turned on by mistake. |
| Demand Rate on SIF | Estimated to be 2.48 per year. The HV is expected to be operated once per working day. There are 248 working days per year. Operator (trained, following written procedures) is expected to make one mistake per 100 operations. |
| Trip Points | Access key not returned / removal |
| Success Criteria | HV is OFF (or prevented from being turned on) due to power supply being isolated. |
| Functional Relationship (Between Input and Output) | HV OFF upon removal of access key. |
| **Common Cause Failures** |
| Electrical Power Loss | System is safe as HV will be off upon power loss. |
| Compressed Air Loss | N/A |
| Hydraulic Pressure Loss | N/A |
| **Process Details** |
| Safe State Definition | HV is powered off. |
| Hazards from Concurrent Safe States | None identified. |
| Process Safety Time | About 4 seconds |
| Requirement to Survive a Major Accident | None identified. Loss of power due to major accidents will put system in safe state. |
| **SIL Data** |
| Mode of Operation | High Demand |
| SIL | Target | SIL 2 | Achieved | SIL 2 |
| PFD / PFH | Target | 1.1E-07/hr | Achieved | 5.3E-08/hr |
| Spurious Trip Rate (/hr) | Target | No availability requirement for PSS0 | Achieved | N/A |
| Target Proof Test Interval (Months) | Sensor Subsystem | Final Element Subsystem |
| Key switch | 24 | Contactor  | 24 |
|  |  | Contactor  | 24 |
| Mean Repair Time (hours) | Sensor Subsystem | Final Element Subsystem |
| Key switch | 8 | Contactor  | 8 |
|  |  | Contactor  | 8 |
| SIF Response Time Achieved | < 2 seconds (total time from detection to system in safe state, including PLC scanning time, and delay to allow BPCS to achieve normal shutdown) |
| **Trip Actions** |
| Manual Shutdown Requirements | ISrc HV OFF is provided via a pushbutton. The process can also be shut down via BPCS. |
| Energise / De-Energise To Trip | De-energise to trip |
| Requirements for Resetting after Shutdown | The HV power supply needs to be manually reset following a shutdown. |
| Overrides / Inhibits / Bypasses (including control measures for when these are in use) | There are no overrides / inhibits / bypasses for this SIF. |
| Dangerous Combinations of Output States | None identified. |
| Actions to Achieve / Maintain Safe State | Ensure power supply to HV is isolated. |
| Action on Valve Discrepancy | N/A |
| **Desired Responses to SIF Failure Modes Properties** |
| Sensor Failures | Fail to correctly read key switch position |
| Logic Solver Failures | Fail to initiate action |
| Final Element Failures | Fail to open relay / contactor |
| **Maintenance Issues** |
| Maintenance Considerations | Maintenance shall be conducted as per device manuals and project operation and maintenance procedures. |

### PSS0\_SIF04 – Door lock – PSS0 Key Exchange

|  |
| --- |
| SIF Details |
| SIF Tag | PSS0\_SIF04 |
| Drawing Number | N/A |
| Hazardous Event | Hazard\_003 IE\_01, Electric shock from attempted access to PSS0 controlled area while HV is ON. |
| SIF Description | Upon detecting access key is in key exchange switch (position ON), lock the Access Door (de-energising 1oo1 solenoid) via a safety PLC (1oo1, red train only). |
| Sources of Demand | Human error, attempting to access PSS0 controlled area whilst HV is on. |
| Demand Rate on SIF | The electric door lock is operated every time HV is turned on. |
| Trip Points | Access key in key exchange switch (position ON) (Safety Key locked in place, mechanical lock engaged). |
| Success Criteria | Access door is electronically locked. |
| Functional Relationship (Between Input and Output) | Electric lock of Access Door upon returning the Access Key to key exchange switch (position ON). |
| **Common Cause Failures** |
| Electrical Power Loss | Electric lock will fail, but system is safe as HV will be off upon power loss. |
| Compressed Air Loss | N/A |
| Hydraulic Pressure Loss | N/A |
| **Process Details** |
| Safe State Definition | Access Door is locked (preventing access when HV is ON). |
| Hazards from Concurrent Safe States | None identified. |
| Process Safety Time | About 4 seconds. |
| Requirement to Survive a Major Accident | None identified. Loss of power due to major accidents will put system in safe state. |
| **SIL Data** |
| Mode of Operation | High Demand (the electric lock will be engaged prior to starting up HV every time). |
| SIL | Target | SIL 2 | Achieved | SIL 2 |
| PFD / PFH | Target | 1.1E-07/hr | Achieved | 1.1E-07/hr |
| Spurious Trip Rate (/hr) | Target | No availability requirement for PSS0 | Achieved | N/A |
| Target Proof Test Interval (Months) | Sensor Subsystem | Final Element Subsystem |
| Key switch | 24 | Solenoid lock | 24 |
|  |  |  |  |
| Mean Repair Time (hours) | Sensor Subsystem | Final Element Subsystem |
| Key switch | 8 | Solenoid lock | 8 |
|  |  |  |  |
| SIF Response Time Achieved | **<**1 second |
| **Trip Actions** |
| Manual Shutdown Requirements | ISrc HV OFF is provided via a pushbutton. The process can also be shut down via BPCS. |
| Energise / De-Energise To Trip | De-energise to lock. |
| Requirements for Resetting after Shutdown | No need to reset after system shutdown. |
| Overrides / Inhibits / Bypasses (including control measures for when these are in use) | There are no overrides / inhibits / bypasses for this SIF. |
| Dangerous Combinations of Output States | None identified. |
| Actions to Achieve / Maintain Safe State | Access door remain electrically locked. |
| Action on Valve Discrepancy | N/A |
| **Desired Responses to SIF Failure Modes Properties** |
| Sensor Failures | Fail to correctly read key switch position |
| Logic Solver Failures | Fail to initiate action |
| Final Element Failures | Fail to de-energise |
| **Maintenance Issues** |
| Maintenance Considerations | Maintenance shall be conducted as per device manuals and project operation and maintenance procedures. |

# Glossary

| Term | Definition |
| --- | --- |
| /hr | Per hour |
| BPCS | Basic Process Control System |
| DO | Digital Output |
| ERIC | European Research Infrastructure Consortium |
| ESS | European Spallation Source |
| FAT | Factory Acceptance Test |
| HAZAN | Hazard Analysis |
| HAZID | Hazard Identification |
| HAZOP | Hazard and Operability |
| HV | High Voltage |
| ICS | Integrated Control System |
| IE | Initiating Event |
| IEC | International Electrotechnical Commission |
| ISrc | Ion Source |
| LEBT | Low Energy Beam Transport |
| LOPA | Layers of Protection Analysis |
| MRT | Mean Repair Time |
| N/A | Not Applicable |
| O&M | Operation and Maintenance |
| PFD | Probability of Failure on Demand |
| PFH | Frequency of failure per hour |
| PLC | Programmable Logic Controller |
| PSS | Personnel Safety System |
| SIF | Safety Instrumented Function |
| SIL | Safety Integrity Level |
| SIS | Safety Instrumented System |
| SRS | Safety Requirement Specification |

# references

1. ESS-0231390: PSS0 SIL Assessment Report.
2. IEC 61511: 2016, Functional safety – Safety instrumented systems for the process industry sector.
3. ESS-0118213: Hazard and risk assessment of the Ion Source and LEBT.
4. ESS-0414418: PSS0 Overall Safety Requirements.
5. ESS-0229491: PSS0 Hazard Register.
6. ESS-0233615: PSS0 Validation and Verification Plan.
7. ESS-0237557: PSS0 Software Planning Document.
8. ESS-0237967: PSS0 Hardware Design Requirements Specifications.

Document Revision history

| Revision | Reason for and description of change | Author | Date |
| --- | --- | --- | --- |
| 1 | First issue | Fan Ye | 2018-02-07 |
| 2 | Updated to align with the latest PSS0 hazard and risk analysis document, and the PSS0 overall safety requirements and their allocation. | Fan Ye | 2018-05-21 |
| 3 | Updated to align with the latest PSS0 SIL Assessment Report. | Fan Ye | 2018-11-07 |
|  |  |  |  |