Document Type	Design Specification
Document Number	ESS-0238059
Date	Feb 7, 2018
Revision	1 (1)
State	Review
Confidentiality Level	Internal
Page	1 (12)

IEC 61508 Safety Requirements Specification Document for PSS0

	Name	Role/Title
Owner	Fan Ye Denis Paulic	PSS Safety Engineer, Isograph Expert, Engineering Safety Consultants Limited, UK Deputy Group Leader for Protection System Group, ICS
Reviewer	Stuart Birch	Senior Engineer – Personnel Safety Systems, ICS
Approver	Annika Nordt	Group Leader for Protection System Group, ICS

TABLE OF CONTENT PAGE

LIST OF TABLES

LIST OF FIGURES

1. SCOPE

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).

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. ISSUING ORGANISATION

ICS Division, ESS ERIC.

3. INTRODUCTION

3.1. General

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

It includes specification of both the functional and safety integrity requirements based upon information provided by ESS PSS Team.

3.2. Scope

This document covers Safety Lifecycle Phase 9 from IEC 61508 [2]: E/E/PE system safety requirements specification, and Phase 3 of IEC 61511 [3].

Figure 1 presents an overview of the IEC 61511 [3] Functional Safety Assessment lifecycle. The highlighted block in this diagram indicates the phase applicable to this document.

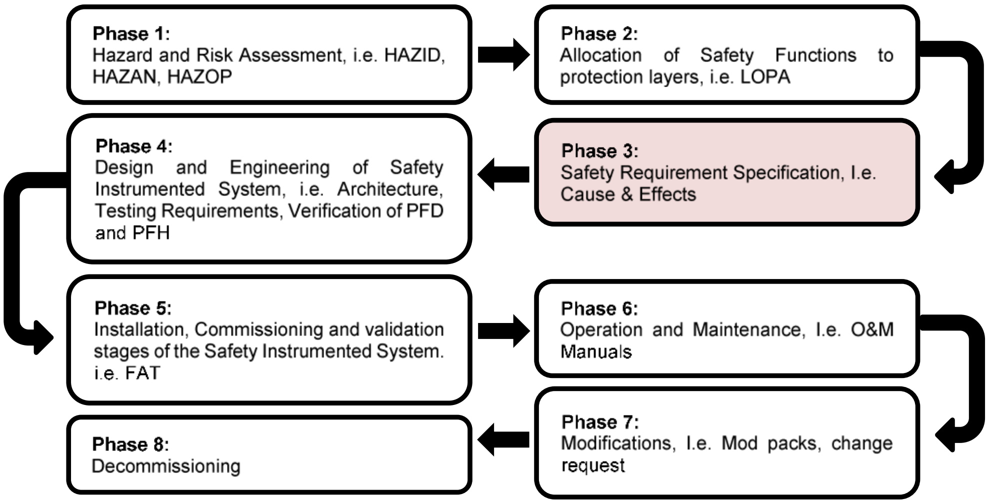
Phase 1:
Hazard and Risk Assessment, i.e. HAZID, HAZAN, HAZOP
Phase 2:
Allocation of Safety Functions to protection layers, i.e. LOPA
Phase 3:
Safety Requirement Specification, I.e. Cause & Effects
Phase 4:
Design and Engineering of Safety Instrumented System, i.e. Architecture, Testing Requirements, Verification of PFD and PFH
Phase 5:
Installation, Commissioning and validation stages of the Safety Instrumented System. i.e. FAT
Phase 6:
Operation and Maintenance, I.e. O&M Manuals
Phase 7:
Modifications, I.e. Mod packs, change request
Phase 8:
Decommissioning

Figure 1: IEC 61511 Functional Safety Assessment Lifecycle Diagram.

The scope of this study was limited to the SIFs identified by the PSS0 Hazard and Risk Analysis (see document ESS-0299506 [1]) supported by the PSS0 Hazard Register [4], and the PSS0 Overall Safety Requirements and their Allocation (see document ESS-0231390 [5]) produced by ESS PSS Team, which incorporates the Safety Integrity Level (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	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
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 has been treated as part of administrative control and excluded from any further assessment.

3.3. 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 4.1 whilst the SRS for each identified SIF is presented in Section 4.2.

4. SAFETY REQUIREMENT SPECIFICATION

4.1. 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	SIS sends signal to BPCS PLC (hard-wired from Red train DO module) to shutdown HV, and with a delay of 1 second. SIS also sends the "PSS OK" status signal to BPCS PLC (hard-wired from Red train DO module) to inform operators in Local control room about 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: 1 second.
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 system is not used during normal operation.
Requirements for process variable validation and handling of bad process variables	Addressed in Verification and Validation Procedure document [6]

Requirements for communication interfaces	No special 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 analysis will not be conducted for PSS0, but security measures will be taken into account. PSS0 will be stand-alone, and can only be accessed locally from a PSS laptop.
Environmental Conditions	
Design requirements	Will be addressed in PSS0 Hardware Design Requirements Specifications [8].

4.2. SRS for the SIFs

4.2.1. SIF01 – PSS0 Emergency Stop

SIF Details				
SIF Tag	SIF01			
Drawing Number	N/A			
Hazardous Event	This was not designed for safety, rather it is for emergency situations such as fire or explosion within PSS0 controlled area, to protect equipment from damage.			
SIF Description	Upon detecting emergency shutdown pushbutton being pressed, shutdown HV by removing its power supply (1oo2 relay and contactor) via 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	Emergency shutdown pushbutton being pressed			
Success Criteria	HV is OFF due to power supply being isolated			
Functional Relationship (Between Input and Output)	HV OFF upon pressing the emergency shutdown pushbutton.=.			
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	

	Emergency shutdown pushbutton	24	Contactor and relay	24
			Contactor and relay	24
Mean Repair Time (hours)	Sensor Subsystem		Final Element Subsystem	
	Emergency shutdown pushbutton	8	Contactor and relay	8
			Contactor and relay	8
SIF Response Time Achieved	N/A			
Trip Actions				
Manual Shutdown Requirements	The process can be shutdown 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 pushbutton 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.			

4.2.2. SIF02 – HV interlock upon intrusion to PSS0 controlled area

SIF Details	
SIF Tag	SIF02
Drawing Number	N/A
Hazardous Event	HAZ003 IE01, Electric shock from attempted access to PSS0 controlled area while HV is ON.
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).
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 gate 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 gate.
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	Estimated to be around 4 seconds. Will be clarified in next version of this document.			
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 3
PFD / PFH	Target	1.0E-03	Achieved	7.7E-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 and relay	24
	Mechanical switch	24	Contactor and relay	24
Mean Repair Time (hours)	Sensor Subsystem		Final Element Subsystem	
	Magnetic switch	8	Contactor and relay	8
	Mechanical switch	8	Contactor and relay	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	Emergency stop is provided via a pushbutton; the process can also be shutdown 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.			

4.2.3. SIF03 – HV interlock – PSS0 Key Exchange

SIF Details	
SIF Tag	SIF03
Drawing Number	N/A
Hazardous Event	HAZ003 IE02, Electric shock when HV is turned on by mistake.

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.			
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	Estimated to be around 4 seconds. Will be clarified in next version of this document.			
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	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	Contactor and relay	24
			Contactor and relay	24
Mean Repair Time (hours)	Sensor Subsystem		Final Element Subsystem	
	Key switch	8	Contactor and relay	8
			Contactor and relay	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	Emergency stop is provided via a pushbutton; the process can also be shutdown 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.

4.2.4. SIF04 – Door lock – PSS0 Key Exchange

SIF Details				
SIF Tag	SIF04			
Drawing Number	N/A			
Hazardous Event	HAZ003 IE01, Electric shock from attempted access to PSS0 controlled area while HV is ON.			
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).			
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 removed from Slot 2 (Safety Key locked in place, mechanical lock engaged)			
Success Criteria	Access gate is electronically locked			
Functional Relationship (Between Input and Output)	Electric lock of Access Gate upon removal of Access Key from Slot 2.			
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 Gate is locked (preventing access when HV is ON).			
Hazards from Concurrent Safe States	None identified.			
Process Safety Time	Estimated to be around 2 seconds. Will be clarified in next version of this document.			
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	6.0E-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	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	Emergency stop is provided via a pushbutton; the process can also be shutdown 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 gate 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.			

5. GLOSSARY

Term	Definition
/hr	Per hour
BPCS	Basic Process Control System
ERIC	European Research Infrastructure Consortium
ESS	European Spallation Source
HV	High Voltage
IEC	International Electrotechnical Commission
MRT	Mean Repair Time
PFD	Probability of Failure on Demand
PFH	Frequency of failure per hour
PSS	Personnel Safety System
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirement Specification

6. 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] ESS-0231390: PSS0 Overall Safety Requirements and their Allocation Document.
[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