IEC 61508 CONCEPT DOCUMENT FOR THE ACCELERATOR PERSONNEL SAFETY SYSTEM 0

	Name	Role/Title
Owner	Stuart Birch	ICS - Senior Engineer - Personnel Safety Systems for Protection Systems Group
Reviewer	Edgar Sargsyan Jörgen Mattsson Annika Nordt Michael Plagge	Accelerator Division - Section Leader Front End & Magnets ESH - Electrical Safety Engineer ICS - Group Leader for Protection Systems Group ESH - Occupational Health & Safety Engineer
Approver	Peter Jacobsson	ESH - Head of Safety, health and environment division

TABLE OF CONTENT PAGE

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

This document provides a concept for the European Spallation Source (ESS) personnel safety system 0 (PSS0) which is needed to operate the Ion Source (ISrc) and Low energy beam transport (LEBT) safely as a test stand for the ESS project in Lund, Sweden. The PSS0 system will prevent access to the Ion Source test stand PSS0 controlled area whilst the electrical hazard(75kV) is present.
The objective of this document is to develop a level of understanding of the Ion Source test stand and its physical environment, sufficient to enable subsequent parts of the safety life cycle to be carried out in accordance with IEC61508:2010[1], Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety Related Systems. The concept document covers safety life cycle stage 1 of IEC 61508 part 1 and is part of the analysis phase of the documentation.
The PSS0 will cover the ISrc safety fence gate and the PSS0 controlled area within the fence see figure 4.

1. ABBREVIATIONS

ALARA	As Low As Reasonably Achievable
AP	Application Program
BIS	Beam Interlock System
E/E/PE	Electrical/Electronic/Programmable Electronic safety related systems
ESS	European Spallation Source
EUC	Equipment Under Control
HV	High Voltage
ISrc	Ion Source
LEBT	Low Energy Beam Transport
LINAC	Linear Accelerator
ODH	Oxygen Deficiency Hazard
PSS	Personnel Safety System
PSS0	Personnel Safety System for ISrc and LEBT Test Stand
QRA	Quantitative Risk Analysis
RF	Radio Frequency
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SSC	Structure, System and Components
SSM	Strålsäkerhetsmyndigheten (Swedish Radiation Safety Authority)

2. INTRODUCTION

2.1. Scope

The scope of this document is limited to the PSS0. The document addresses the requirements of IEC61508 safety lifecycle phase 1 and the scope of this document is defined by (but not limited to): IEC61508: 2010 Part 1 section 7.2 Concept.

2.2. Objectives

This document details the concept of the PSS0 and the objective of this document is to detail the system's physical environment, the likely hazards and hazardous events arising from operation of the ISrc, LEBT and its accompanying equipment, the safety regulations that apply and any relevant details of interactions with other systems. In line with IEC61508-1: 2010 clause 7.2.1. This document will also develop a high level of understanding of the equipment under control (EUC) sufficient to enable other lifecycle activities to be satisfactorily carried out and detail lifecycle documentation that will be produced through the development of the safety systems.

2.3. IEC61508 Lifecycle

IEC 61508:2010 is an international standard concerned with functional safety achieved by safety related systems that are primarily implemented in Electrical/Electronic and/ Programmable Electronic technologies (E/E/PE). The PSS0 is an example of this, and will fall within the scope of IEC 61508:2010. This standard provides an overall safety lifecycle structure for functional safety as detailed in Figure 1 and ESS will follow this lifecycle.
All hardware devices used in the PSS0 system will be standard devices using proven 'commercial off the shelf' technology and all application programs (AP) will be developed in accordance with IEC61511:2016.
This document will form part of the analysis section of the IEC61508 overall safety lifecycle and a high-level list of IEC61508 lifecycle documentation will be listed in Table 1 of this concept document.
To be able to complete the overall safety requirements, a hazard and risk analysis shall be undertaken for the Ion source related Equipment Under Control (EUC). This will be completed by the PSS Team, the ion source and LEBT system designers and stakeholders. After hazard identification and analysis of the safety functions, a decision will be made on the risks that the PSS0 systems have to mitigate against and to reduce these risks to an acceptable level, the PSS Team will use the ALARA principle and a safety requirements allocation will then be formulated. IEC 61508:2010 is only concerned with functional safety achieved by systems that are primarily implemented in Electrical / Electronic and / Programmable Electronic technologies (E/E/PE).
To be able to calculate the Safety Integrity Level (SIL) that PSS0 functions should be designed to, all risk reduction methods shall be understood and calculations documented.

Hazard and risk analysis techniques will include qualitative and quantitative methods.

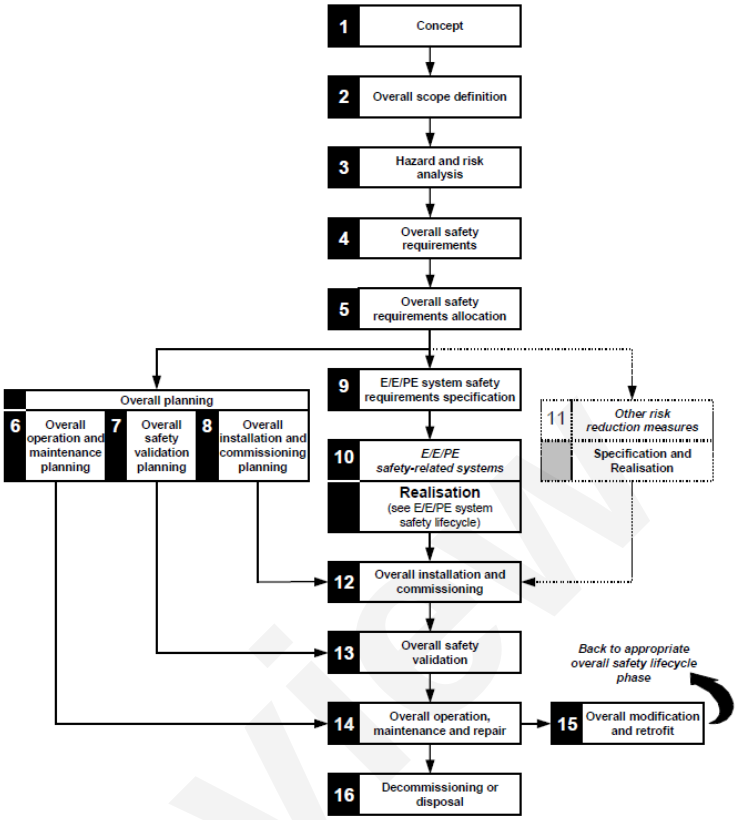

Figure 1: IEC 61508 overall safety life cycle.

As part of the overall safety lifecycle, a full set of approved documents with full IEC61508 compliance will be authored. Table 1 addresses the documents required for the analysis phase of the safety system safety lifecycle, and describes their objectives. The table also details the document inputs and outputs for each stage of the lifecycle. Table 2 addresses the documents required for the realisation phase of the safety lifecycle.

IEC61508 safety lifecycle phase.	Title	Objectives	Inputs	Outputs
1	**Concept**	To develop a level of understanding of the EUC and its environment sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.	All relevant information necessary to meet the requirements of the sub clause.	Information concerning the EUC, its environment and hazards.
2	**Overall Scope**	To determine the boundary of the EUC and the EUC control system; To specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc.).	Information concerning the EUC, its environment and hazards.	Defined scope of the hazard and risk analysis.
3	**Hazard and risk analysis**	To determine the hazards, hazardous events and hazardous situations relating to the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances, including fault conditions and reasonably foreseeable misuse. To determine the event sequences leading to the hazardous events. To determine the EUC risks associated with the hazardous events.	Defined scope of the hazard and risk analysis.	Description of, and information relating to, the hazard and risk analysis.
4 & 5	**Safety requirements and their allocation**	To develop the specification for the overall safety requirements, in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems and other risk reduction measures, in order to achieve the required functional safety. To allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety related systems and other risk reduction measures; To allocate a safety integrity level to each safety function to be carried out by an E/E/PE safety-related system.	Description of, and information relating to, the hazard and risk analysis. Specification of the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements.	Specification of the overall safety requirements in terms of the safety functions requirements and the safety integrity requirements. Information on the allocation of the overall safety functions, their target failure measures, and associated safety integrity levels. Assumptions made concerning other risk reduction measures that need to be managed throughout the life of the EUC.

Table 1: Analysis phase documents.

IEC61508 safety lifecycle phase.	Title	Objectives	Inputs	Outputs
6	**Overall operation and maintenance planning**	To develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance.	Information on the allocation of the overall safety functions, their target failure measures, and associated safety integrity levels Assumptions made concerning other risk reduction measures that need to be managed throughout the life of the EUC.	A plan for operating and maintaining the E/E/PE safety-related systems.
7	**Overall safety validation planning**	To develop a plan for the overall safety validation of the E/E/PE safety-related systems.	Information and results of the overall safety requirements allocation.	A plan for the overall safety validation of the E/E/PE safety-related systems.
8	**Overall installation and commissioning planning**	To develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure that the required functional safety is achieved; To develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure that the required functional safety is achieved.	Information and results of the overall safety requirements allocation.	A plan for the installation of the E/E/PE safety-related systems; A plan for the commissioning of the E/E/PE safety-related systems.
9	**E/E/PE system safety requirements specification**	To define the E/E/PE system safety requirements, in terms of the E/E/PE system safety functions requirements and the E/E/PE system safety integrity requirements, in order to achieve the required functional safety.	Information and results of the overall safety requirements allocation.	Specification of the E/E/PE system safety requirements.
11	**Other risk reduction measures: specification and realisation**	To create other risk reduction measures to meet the safety functions requirements and safety integrity requirements specified for such systems (outside the scope of this standard).	Other risk reduction measures safety requirements specification (outside the scope and not considered further in this standard).	Realisation of each other risk reduction measure according to the safety requirements for that measure.

Table 2: Realisation phase documents.

2.4. IEC61511 Application Program Development.

All PSS0 application programming will be developed in accordance with IEC 61511-1 (2017) Clause 12 and in particular:

- Clause 12.2 Application program general requirements
- Clause 12.3 Application program design
- Clause 12.4 Application program implementation
- Clause 12.5 Application program verification

3. CONCEPT REQUIREMENTS FOR PSS0

3.1. Physical Location

The European Spallation Source ERIC facility is being constructed on a green field site on the borders of Lund in Sweden. Figure 2 shows a map showing the site position. The visiting address is PO box 176, SE-221 00, Lund, Skåne, Sweden.

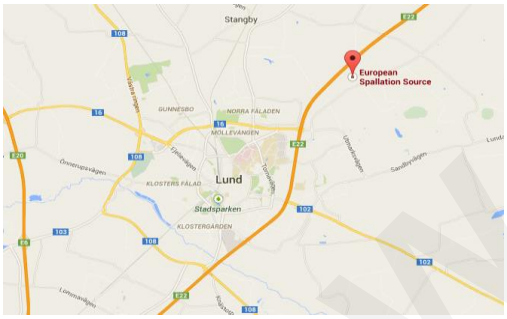

Figure 2: European Spallation Source ERIC Site.

3.2. Description

3.2.1. ESS

The European Spallation Source (ESS), currently under construction, will be a multi-disciplinary research Centre located in Lund/Sweden, enabling researchers from academia and industry to performing fundamental and applied research using neutron beams. The facility consists of a 600m long linear Accelerator (LINAC) composed of a normal conducting section from the ion source to the end of the Drift Tube Linac (DTL) and a superconducting section, which includes the Spoke cavities, medium beta cavities and high beta cavities. It will allow sending 2.86ms long pulses of 2GeV protons at a 14Hz repetition rate to the rotating, helium-cooled tungsten target. This will produce thermal and cold-moderated neutrons, which are further guided to a large variety of state-of-the-art neutron instruments supported by a suite of laboratories as well as a supercomputing data management and development centre. ESS will be a low-energetic neutron source of unprecedented high brightness and scientific performance delivering the first spallation neutrons in 2020 and reaching its full design specifications in 2025 with a suite of 22 research neutron instruments. (user programs will start in 2023)

3.2.2. ISrc and LEBT

The ISrc and LEBT test stand will be the first system at the ESS facility to produce a proton beam up to and an energy of 75keV

The ISrc and LEBT test stand consists of an ion source on a 75 kV high voltage (HV) platform (the power supply is capable of up to 100kV), and a 2.5m long Low Energy Beam Transport (LEBT) with diagnostics. Figure 3 shows an image of the ISrc and LEBT.

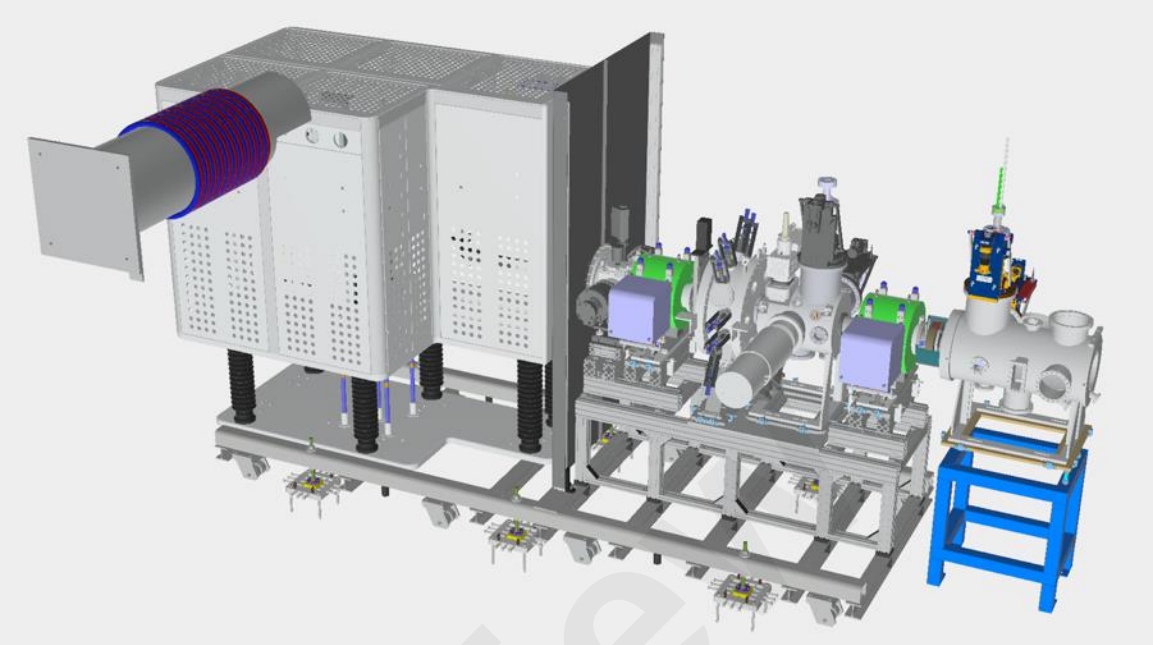

Figure 3: ISrc and LEBT.

The test stand will be installed into the ESS accelerator G01 tunnel (see figure 4) and will have a high voltage ISrc fenced area around the HV platform. This high voltage ISrc Fenced area will be lead lined to provide radiation shielding.

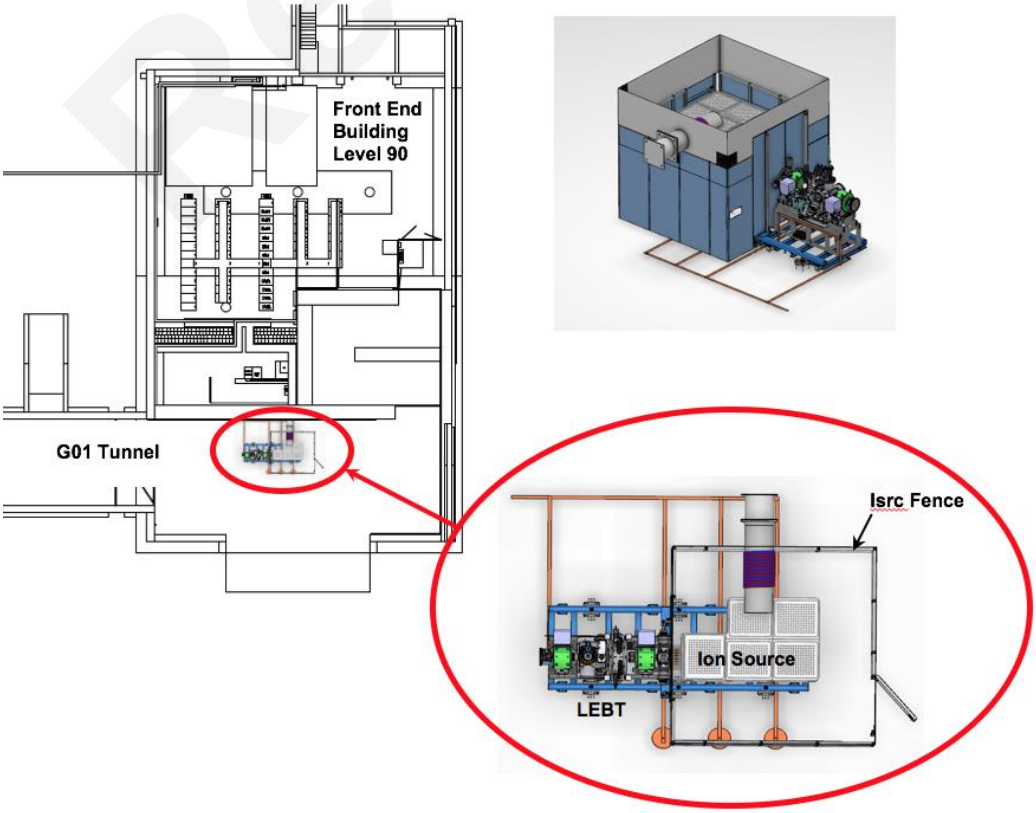

Figure 4: ISrc and LEBT Test Stand location.

The ISrc has a plasma chamber, located on the HV platform, were microwaves will heat hydrogen gas and ionise it to create a plasma. The electric field from the 75 kV bias extracts the positive ions (protons) from the plasma and becomes the proton beam. The beam travels through the two-solenoid LEBT and is dumped on a dedicated beam stop at the end of the commissioning tank, which is after the LEBT faraday cup.

3.3. The Primary Role of PSS0

The primary role of the PSS0 is to protect workers from being harmed by exposure to high voltage (HV) arising when the ISrc and LEBT test stand is energised under all operating modes and lifecycle phases. This will be achieved by preventing the access of personnel to the PSS0 controlled area when a HV hazard is present and allowing safe access when the HV hazard is removed. Figure 5 illustrates a plan view of the PSS0 controlled area (shaded in red). Section 5 will list hazards that will be in the PSS0 controlled area.

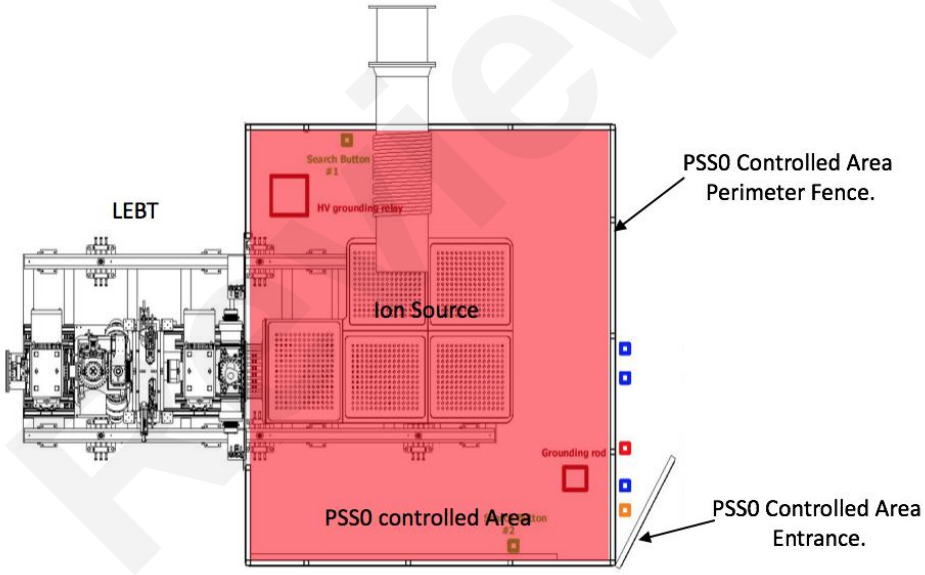

Figure 5: ISrc and LEBT PSS0 Controlled Area.

PSS0 aims to mitigate high voltage electrical hazards for personnel arising from operating the ISrc and LEBT test stand. The high voltage platform also has a three-phase 400V incoming supply which goes through a 400V isolation (75kV working isolation) transformer this will feed the main plasma circuits on the ion source.
The PSS0 system design is chosen to suit the requirements in Swedish standard SS-4364000: Low-voltage electrical installations - Rules for design and erection of electrical installations [3].
The system operation is chosen to suit the requirements in SS-EN 50110-1:2013, a European standard for operation of electrical installations [4].

3.4. Ion source Equipment Under Control

After hazard identification of the ISrc and its associated systems, the Equipment Under Control (EUC) will be primarily made up of systems, devices and components that are used in the acceleration process from the ion source through to the last component in the LEBT. Table 3 lists the expected EUC that will have an interface with PSS0.

EUC	PSS0
ISrc HV power supply	X
ISrc Safety Fence gate	X
ISrc HV Platform enclosure door switches	X

Table 3: Ion Source EUC.

All EUC interfaces with PSS0 will be fully documented and approved.

4. PSS0 SOURCES OF HAZARDS

PSS0 shall mitigate against the following hazards inside the PSS0 controlled area before any workers are permitted to enter:

- Electrical hazard from the high voltage power supply.

There is also a 400V three phase isolation transformer (rated for 75kV isolation and insulation) which will feed circuits within the high voltage platform. All safety for these circuits will be mitigated against by using the ESS standard lock out tag out procedures at the main circuit board on the HV platform.

Electrical hazards are identified in accordance with standard Swedish authority's voltage hazard categories. Table 4 lists the three main voltage categories described in the Swedish standards and regulations.
All electrical hazards will be assessed and risk assessments carried out on all systems with a voltage > 50VAC (or 120V Ripple Free DC). The results will determine whether the system will require added local protection (i.e. terminal covers and protection) or, have an interface with the E/E/PE PSS system.

Swedish	English	Accelerator PSS
Klenspänning	Extra-low voltage	U < 50V AC (or 120V Ripple Free DC)
Lågspänning	Low voltage	U < 1000V AC (or 1500V DC)
Högspänning	High voltage	Above "lågspänning"

Table 4: Swedish authority voltage hazard categories.

4.1. Safety Matrix

PSS0 safety hazards shall be identified and assessed using the matrix in Table 5.

			Consequence				
			Negligible	Minor	Major	Hazardous	Catastrophic
Likelihood			A	B	C	D	E
Frequent	1	$>10^{-2}$	1A	1B	1C	1D	1E
Occasional	2	$>10^{-3} \leq 10^{-2}$	2A	2B	2C	2D	2E
Remote	3	$>10^{-4} \leq 10^{-3}$	3A	3B	3C	3D	3E
Improbable	4	$>10^{-6} \leq 10^{-4}$	4A	4B	4C	4D	4E
Highly Improbable	5	$<10^{-6}$	5A	5B	5C	5D	5E

Table 5: Conventional Safety Function Risk Matrix.

Unacceptable	Risk level is unacceptable and risk reduction shall be carried out. Regulatory requirements on acceptable risk level are not met.
Tolerable	Regulatory requirements on acceptable risk level are met. Risk level is tolerable; however, evaluation of the possibility to further reduce risk is recommended.
Acceptable	Risk reduction is not required.

4.1.1. Safety Risk Consequence and Likelihood

A single event can generate a range of consequences which can have both positive and negative effects on safety. Table 6 defines the five categories of PSS consequence for conventional safety functions and outlines a brief description of each of the consequence effects.

Consequence	Description	Value
Negligible	**Few Consequences**	**A**
Minor	**Minor Injury (cuts, scrapes and strains)**	**B**
Major	**Serious Injury (loss of limb, sight etc.)**	**C**
Hazardous	**Single Death**	**D**
Catastrophic	**Multiple Deaths >1**	**E**

Table 6: PSS Conventional Safety Consequences.

Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively. Table 7 defines the five categories of PSS likelihood for conventional safety functions and outlines a brief description of each of the likelihood effects.

Likelihood	Description	Probability	Value
Frequent	**Likely to occur many times (has occurred frequently)**	**$>10^{-2}$**	**1**
Occasional	**Likely to occur sometimes (has occurred infrequently)**	**$>10^{-3}\leq10^{-2}$**	**2**
Remote	**Unlikely to occur, (not known to have occurred)**	**$>10^{-4}\leq10^{-3}$**	**3**
Improbable	**Very unlikely to occur, (not known to have occurred)**	**$>10^{-6}\leq10^{-4}$**	**4**
Highly Improbable	**Almost inconceivable that the event will occur**	**$<10^{-6}$**	**5**

Table 7: PSS Conventional Safety Likelihood.

4.2. Predicted Access rates to the PSS0 Controlled Area

One of the strategies for managing the High voltage hazards in the ISrc PSS0 controlled area is by preventing access into the area whilst the hazard is present. The predicted access rates to the PSS0 controlled area are shown in Table 8.

Access	Description
Maximum number of operational days for the test stand	**A maximum of 248 days**
Access during an operational day	**Entry into PSS0 controlled area 2 times per day.**
Access during shutdown	**Constant (PSS0 controlled area opened)**

Table 8: PSS0 controlled area predicted access rates.

5. PSS0 INTERFACES

In addition to the ISrc EUC, PSS0 will be required to interface with other systems at ESS, and some of these systems will not be developed in accordance with IEC 61508:2010. The following list of systems (but not limited to) will potentially interface with PSS0:

- The control system (EPICS based system),

All interfaces with PSS0 will be fully documented and approved.
All hardware devices used in the PSS0 systems will be standard commercial off the shelf devices using proven technology and the application program will be developed in accordance with IEC61511:2016.

6. PSS0 SAFETY REGULATIONS

The following list of safety regulations and European Spallation Source ERIC documents shall be used as guidance in conjunction with the design and development of the PSS0.

- IEC 61508:2010: Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems. [1]
- IEC 61511:2016 Functional safety - Safety instrumented systems for the process industry sector.
- Swedish Work Environment Act (AML). As detailed by the Swedish Work Environment Authority: http://www.av.se/inenglish/ .[2]

7. REFERENCES

[1] IEC61508:2010 Part 0 – Part 7. Functional Safety of electrical/electronic/programmable electronic safety-related systems. CENELEC Ref. No EN 61508-1:2010E

[2] Swedish Work Environment Act (AML). As detailed by the Swedish Work Environment Authority: http://www.av.se/inenglish/ .

[3] Swedish standard SS-4364000: Low-voltage electrical installations - Rules for design and erection of electrical installations
[4] The system operation is chosen to suit the requirements in SS-EN 50110-1:2013, a European standard for operation of electrical installations

8. DOCUMENT REVISION HISTORY

Revision	Reason for and description of change	Author	Date
1	First issue.	Stuart Birch	2018-01-08