IEC 61508 HAZARD AND RISK ANALYSIS DOCUMENT FOR PSS0

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

TABLE OF CONTENT PAGE

LIST OF TABLES

LIST OF FIGURES

1. EXECUTIVE SUMMARY

This report describes the hazard and risk analysis for the Personnel Safety System 0 (PSS0). PSS0 is required for operation of the Ion source (ISrc) and Low energy beam transport (LEBT) of the Accelerator as test stand and will prevent access to the Ion source test stand (HV safety fence, PSS0 controlled area) if any electrical hazard is present. It will also ensure that hazardous equipment cannot be powered during access to the PSS0 controlled area.

1.1. Objectives

The objective of this document is to determine the hazards, hazardous events and hazardous situations for all reasonably foreseeable circumstances, including fault conditions and reasonably foreseeable misuse of the system in accordance with IEC 61508 [1]; and to determine the event sequences and Equipment Under Control (EUC) risks leading to the hazardous events.

The hazard identification (HAZID) was carried out through the official HAZID meeting with the ISrc and LEBT system designers and stakeholders and representatives from the ESS Environment, Safety and Health (ESH) Division. All discussions and conclusions from that meeting are documented as meeting minutes, which are used as a proof for carried out HAZID.

After HAZID and defining hazardous situations and initiating events relevant to PSS0, as well as the other reduction methods that can affect mitigation of the consequences, the hazard analysis (HAZAN) was performed by updating the hazard register and performing the Event Tree Analysis (ETA).

1.2. Results

The minutes from HAZID meeting are available in ESS-0236105 [10].

Latest version of PSS0 Hazard register can be found in ESS-0229491 [11].

2. ABBREVIATIONS

ALARA	As Low As Reasonably Achievable
BNC	Bayonet Neill–Concelman
BPCS	Basic Process Control System
E/E/PE	Electrical/Electronic/Programmable Electronic
EMU	Emittance Measuring Unit
ESS	European Spallation Source
EUC	Equipment Under Control
ESH	Environment, Safety and Health
ETA	Event Tree Analysis
FSA	Functional Safety Assessment
HAZAN	Hazard Analysis
HAZID	Hazard Identification
HV	High Voltage
ID	Identifier
IE	Initiating Event
INFN	Istituto Nazionale di Fisica Nucleare
ISrc	Ion Source
LEBT	Low Energy Beam Transport
LINAC	Linear Accelerator
LOPA	Layers Of Protection Analysis
LOTO	Lockout Tag-Out
O&M	Operation and Maintenance
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PLC	Programmable Logic Controller
PS	Power Supply
PSS	Personnel Safety System
PSS0	Personnel Safety System 0
SIF	Safety Instrumented Functions
SIL	Safety Integrity Level
SSM	Strålsäkerhetsmyndigheten (Swedish Radiation Safety Authority)

3. INTRODUCTION

3.1. Objectives

The main objective of this hazard and risk analysis report is to describe the hazard and risk analysis techniques used for PSS0, utilising mainly qualitative methods to identify the hazards and perform risk analysis. As defined in the IEC 61508 standard [1], the report has the following objectives:

- To determine the hazards, hazardous events and hazardous situations relating to the Equipment Under Control (EUC[1]) and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances, including fault conditions and reasonably foreseeable misuse (see 3.1.14 of IEC 61508-4);
- To determine the event sequences leading to the hazardous events;
- To determine the EUC risks associated with the hazardous events.

3.2. Scope

This document addresses the requirements of IEC 615108 safety lifecycle Phase 3: “Hazard and risk analysis”; and IEC 61511 [2] Phase 1 of Functional Safety Assessment (FSA) Lifecycle diagram (see Figure 1). PSS0 software design will comply with IEC 61511.

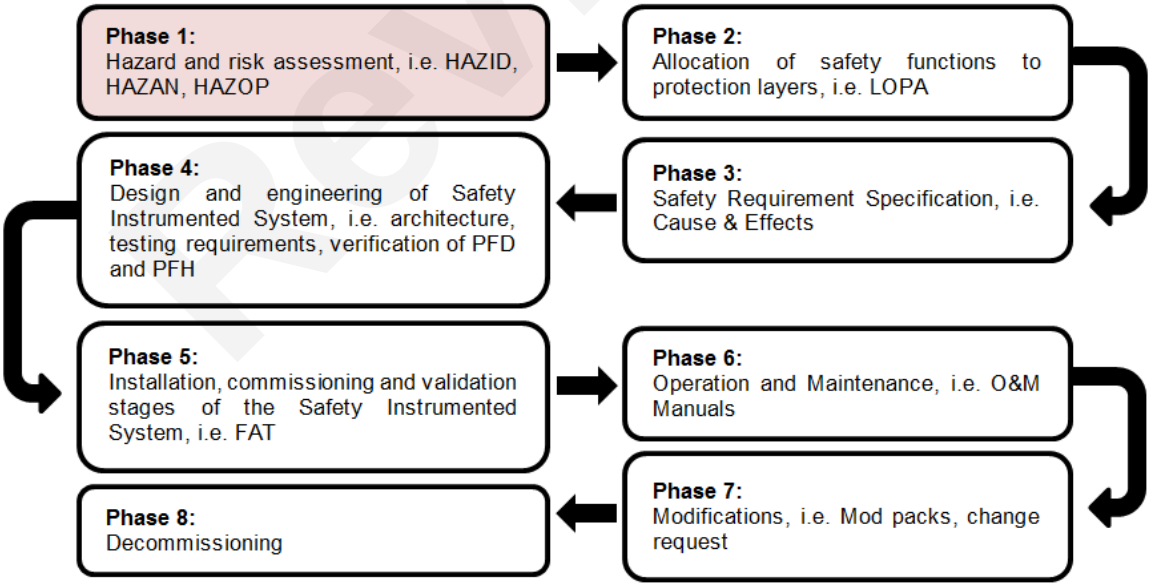


Figure 1: IEC 61511 Functional Safety Assessment Lifecycle Diagram.

The scope of this document is limited to the PSS0. The study assesses the potential risks to the safety of personnel. This report is in continuation to PSS0 IEC 61508 Concept [3] and Scope [4] documents, which address IEC 61508 overall safety life cycle concept, requirements and scope for the analysis phase documents in compliance with IEC 61508:2010 standard. Scope covers following the items:

[1] PSS0 EUC is defined in PSS0 scope document [4].

- Identify hazards and initiating events associated with PSS0 and evaluate the related consequences;
- Develop a hazard register, listing all initiating events including fault conditions and misuse for abnormal and infrequent operation modes
    - Determine event sequences leading to the consequences;
    - Determine the likelihood;
    - Evaluate the risk;

4. HAZARD AND RISK ANALYSIS FOR PSS0

4.1. Requirements

IEC 61508-1 chapter 7.4.2 contains the requirements for hazard and risk analysis briefly explained below:

- A hazard and risk analysis shall be undertaken which shall take into account information from the overall scope definition phase, defined in [4].
- Consideration shall be given to the elimination or reduction of the hazards.
    - This is not completely in the scope of IEC 61508, but highlights the primary importance of identification of hazards and application of inherent safety principles and application of good engineering practice to reduce the risk from the hazards.
- The hazards, hazardous events and hazardous situations of the EUC and the EUC control system shall be determined under all reasonably foreseeable circumstances. This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation of the EUC.
- The event sequences leading to the hazardous events shall be determined, likelihood of the hazardous events shall be evaluated, consequences associated with the hazardous events shall be determined and EUC risk shall be evaluated, or estimated, for each determined hazardous event. These requirements can be met by the application of either qualitative or quantitative hazard, or risk analysis techniques.

4.2. Assumptions

In this hazard and risk analysis, the following assumptions are considered:

- Only the electrical hazard (High Voltage) is considered, as other hazards are not in the scope of PSS0.
- PSS0 controlled area (Section 3.1. in [4]) is hazardous if the Ion Source High Voltage Power Supply (ISrc HV PS) is energised. If a person enters the area when HV PS is powered it is considered fatal. Also, if the ISrc HV PS is de-energised the area is considered safe.
- Only the safety related consequences are taken into account in this document. There may be some other types of consequences, i.e. operational consequences (e.g. decreased availability), but these will not be addressed in the PSS0 analysis.

- The focus is mainly on the operational phase (HV on), but the worst case scenario of shutdown phase is considered, i.e. when the HV PS can be inadvertently started.
- PSS0 is designed in a fail-safe way, meaning that failure of the PSS0 system won't bring the system to hazardous state.
- Due to lack of information in operator instructions and maintenance activities, human actions are not fully credited in this analysis; however, conservative assumptions will be used to estimate human errors and they will be modelled in the IEC61508 Overall Safety requirements and their allocation document [5].
- Human actions during maintenance are considered only in critical procedures, i.e. formalised search process.
- The Human Reliability Analysis (HRA) is not planned in this phase of PSS (PSS0), but will be done for future phases.
- To estimate the component failure data operating experience for similar designs are considered and good engineering practice will be used (e.g. the values recommended by the component manufacturers).
- The safety requirements allocation process will ensure that the common cause, common mode, and systematic failures are sufficiently low compared to the overall risk reduction requirements.

4.3. Methodology

The methodology for hazard and risk analysis for PSS0 is presented in Figure 2 and discussed in detail in the sections below.

Figure 2: Hazard and Risk Analysis Methodology for PSS1.

The methodology for this report is structured in three main analysis parts:

1. Hazard identification, where PSS0 relevant hazards are identified and assumptions are discussed with EUC stakeholders and representatives from ESS Environment, Safety and Health (ESH) division.
2. Hazard register, where identified hazards, hazardous scenarios and initiating events are documented and analysed using the Conventional Safety Risk Matrix

(Section 5.1. in [3]) as a reference; and PSS0 relevant barriers and protection layers are listed.

3. Accident analysis, where progression from initiating event to potential consequences is performed qualitatively using Event Tree Analysis (ETA) modelling and probabilistic methods.

5. HAZARD IDENTIFCATION PROCESS FOR PSS0

The Hazard Identification (HAZID, part 1, clause 8.2.3 in [2]) process is a design-enabling tool, used early in a project as soon as process flow diagrams and operating procedures are available. Normally, the existing site infrastructure, weather, and geotechnical data are also required, these being a source of external hazards. It usually involves brainstorming meetings between designer, system stakeholders (or clients), health and safety representatives, project management and operations personnel. The major findings, decisions and hazard ratings help to deliver safety compliance, and form the input to Hazard Register required by many licensing authorities.

5.1. Meetings important for HAZID process

There were three important meetings to define the requirements, assumptions, hazards and boundaries of PSS0:

- *Visit to Istituto Nazionale di Fisica Nucleare (INFN) Catania*
  - 2017-07-17 – 2017-07-19
  - Purpose: to inspect electrical safety aspects of ISrc and LEBT.
  - Meeting minutes can be found in [6]
  - Result: Defined requirements and design proposals for PSS0.

- *Ion Source HV safety fence and PSS0 design review meeting*
  - 2017-11-01
  - Purpose: to review design of Ion Source safety cage and preliminary design of PSS0.
  - Reference documents:
    - Ion source high voltage safety fence [7]
    - Concept of Operations For the Accelerator Personnel Safety System 0 (PSS0) [8]
  - Meeting minutes can be found in [9];
  - Result:
    - Assumptions for Ion Source HV safety fence and boundaries of PSS0 were defined.
    - Preliminary design of PSS0 was approved.

- *Official HAZID meeting for PSS0*
  - 2018-01-30
  - Purpose:

- Reference documents:
  - IEC 61508 Concept Document for PSS0 [3]
- Meeting minutes can be found in [10]
- Result: PSS0 hazards, hazardous situations and initiating events were identified.

5.2. PSS0 Sources of Hazards

The PSS0 shall mitigate only against electrical hazards, which are identified in accordance with standard Swedish authority's voltage hazard categories (see Table 1). If the voltage is above 50V AC (or 120V Ripple Free DC) it is considered as electrical hazard in PSS0.

Table 1: Electrical hazards according to Swedish authority [13].

Swedish	**English**	**Voltage**
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 "Low voltage"

Table 2 shows the equipment/systems in PSS0 with possibility to cause electrical hazard:

Table 2: PSS0 hazardous equipment/systems.

Equipment / System	**Voltage**	**PSS0 Hazard / Justification**
Ion source high voltage platform	75kV	Yes.
Ion source isolation transformer to supply power to all devices on HV platform	400V AC	No. For any activity within ISrc fenced area (e.g. cleaning, maintaining, etc.) the Lockout Tag-out (LOTO) procedure will be carried out, and adjacent low voltage live parts will be covered. This was agreed with Accelerator Division and is documented in [8]
Two LEBT Repeller electrodes	3,5kV	No. The Repeller electrodes use standard insulated BNC safety high voltage connectors. All cable terminations and live parts will be protected with proper insulation material. The insulation prevents any access/accidental contact with live parts.

Equipment / System	Voltage	PSS0 Hazard / Justification
LEBT chopper	10kV	No. The HV cable will be terminated inside the box above the chopper. There is no specific electrical hazard associated with the chopper, as there is no live part easily accessible by the operators.
LEBT Faraday cup	2kV	No. LEBT Faraday cup is inside the enclosure and it's not reachable. It also uses standard insulated BNC safety high voltage connectors.
LEBT Emittance measurement unit (EMU)	1,5kV	No. LEBT EMU is inside the enclosure and it's not reachable. It also uses standard insulated BNC safety high voltage connectors.

Note: Turning off incoming power (or a mains input power failure) of the isolation transformer can result in failure of multiple devices on the HV platform that are connected to ground/earth. The avoidance of this will be taken into account only in the next phase of PSS.

The predicted access rates to PSS0 controlled area is given in IEC 61508 Concept document [3], Chapter 5.2.

6. HAZARD REGISTER

The conclusion and decisions from above mentioned meetings served as inputs to create the PSS0 Hazard register. It summarizes all initiating events and provides qualitative assessment of hazardous scenarios against Conventional safety risk matrix. Figure 4 illustrates a step-by-step example of filling in (qualitative assessment) the PSS0 Hazard register for initiating event IE01 (see Table 4). A complete version of the PSS0 Hazard register can be found in [11]. Table 3 provides the brief description of the PSS0 Hazard register elements (columns), which are in compliance with IEC 61508 requirements on identification of hazardous events, their likelihoods and consequences;

Table 3: PSS0 Hazard Register elements.

PSS0 Hazard Register column	Description
Hazard ID / IE number	*PSS_Hazard_xxx* - PSS relevant hazard IDs are created to be consistent throughout this sheet and

	reports in all phases of PSS. The IE number identifies the initiating event for given hazard.
Hazard	A definition of PSS relevant hazard. Only one hazard is PSS0 relevant, but this field is kept to be consistent through all phases of PSS.
Initiating Event	An event that can lead to hazardous situation. Identified PSS0 initiating events are leading to PSS0 hazard.
Consequences	Consequences as defined in Conventional Safety Risk Matrix and qualitative evaluation of initiating event scenario.
Likelihood	Evaluated probability of initiating event happening based on qualitative evaluation of initiating event scenario.
Barriers and procedures	A list of barriers and procedures that are in place to prevent and detect the initiating event and its consequences (without PSS0 safety functions in place).
PSS function required Yes/No	Is the PSS0 function required to reduce the risk to tolerable region?
Protection and mitigation	A list of proposed PSS0 safety functions to reach tolerable region.
Human actions	A list of human actions associated with the initiating event and PSS0 functions.
Risk reduction (with PSS functions in place and working)	Qualitative evaluation of how much the risk is reduced while considering PSS0 functions in place and working.
Risk measures independent of PSS	Other risk measures independent to PSS0 but implemented in ESS overall design.
Recommendations and comments	Recommendations and comments from PSS team to be considered further.
Screening IN/OUT	Screened IN initiating events are considered for further analysis. Screened OUT initiating events are analysed only qualitatively and not considered for further analysis. Justification for screening out will be described in this report.

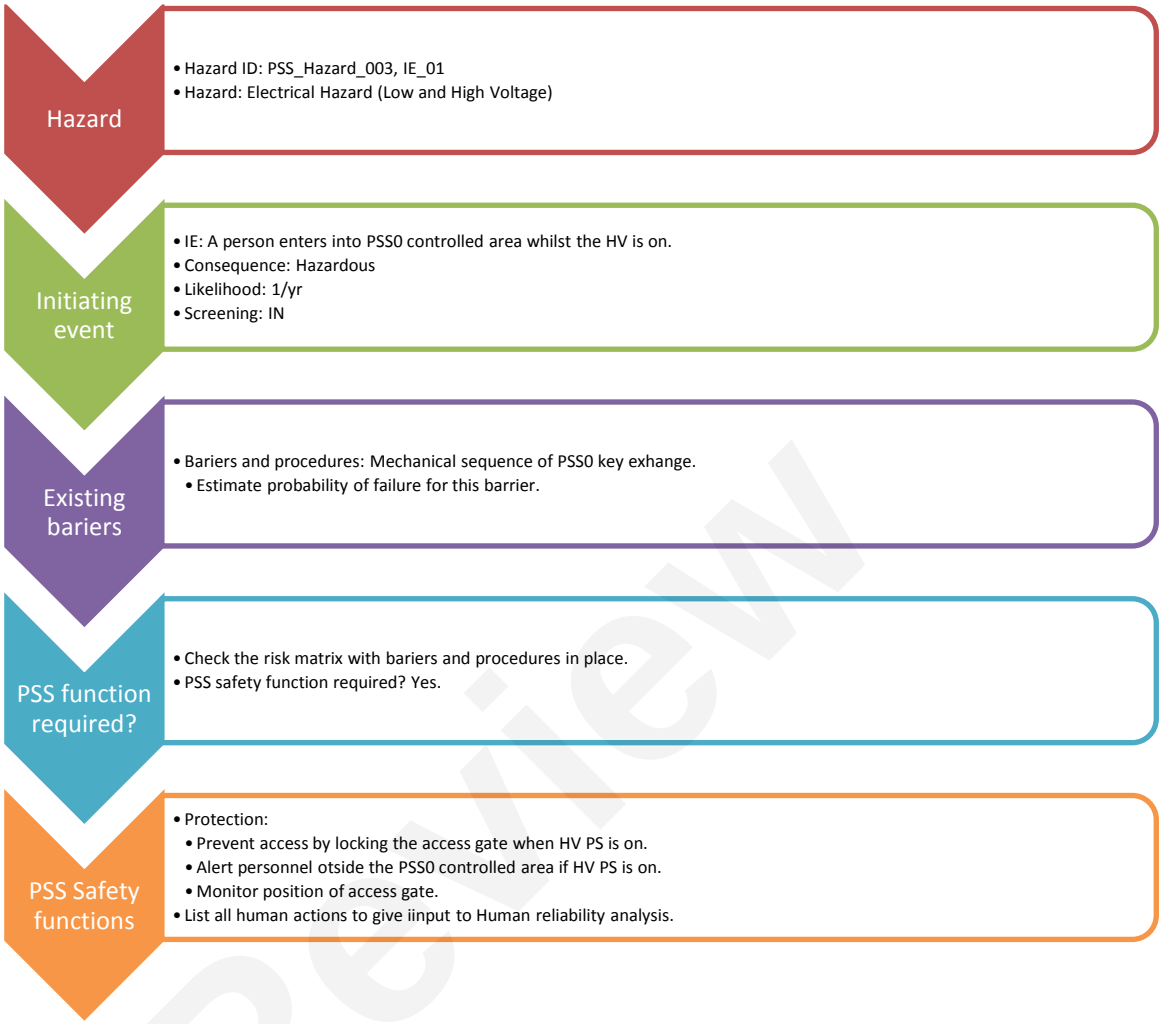


Figure 3: Step-by-step example of filling-in the PSS0 Hazard register for Initiating event IE01.

Hazard ID IE number	Hazard	Initiating Event (IE)	Consequences	Likelihood (Frequency/ Year)	Barriers and procedures	PSS safety function required Yes/No	Protection and Mitigation	Human Actions	Risk Reduction (with PSS0 functions in place and working)	Recommendations and comments	Screening (IN/OUT)
PSS_Hazard_003 IE_01	Electrical Hazard (High Voltage)	A person enters into PSS0 controlled area (Fenced area) whilst the HV is ON.	Hazardous	1.0	1. PSS0 key exchange - mechanical sequence	Yes	1. Prevent access by locking the access gate when HV PS is on 2. Alert personnel outside the fenced area - HV ON light + Blue (Beam ON light) 3. Access gate position monitoring Action: Upon detection of door opening immediately switch-off the mains power to the following systems Ion Source HV PS (Extraction System).	Entry procedure to fenced area (PSS0 controlled area). Exit from PSS0 controlled area.	Tolerable		IN

Figure 4: The example of Initiating event IE01 in PSS0 Hazard register.

6.1. Initiating events

An initiating event for PSS0 is defined as an event that creates a disturbance in PSS0 controlled area and has a potential to lead to a dangerous consequence (e.g. fatality to worker/s entering the PSS0 controlled area). Table 4 shows all initiating events identified in the PSS0 Hazard register, together with estimated likelihoods and justification for chosen values. The risk is evaluated to determine what can go wrong, how likely it is and what the consequences are.

Table 4: PSS0 Initiating Events.

ID/Initiating event	Likelihood	Screening
IE01: A person enters into PSS0 controlled area whilst the HV is ON.	1/yr HV PS is expected to be energised once each day (during 248 working days per year gives frequency of HV ON 248/yr). For this event to happen a person needs to be around the area when HV is energised, come to the access gate and try to break in. Conservatively, the PSS team estimated that person makes mistake here once every 248 operations, which gives estimated likelihood.	IN
IE02: A person is in PSS0 controlled area when HV PS unexpectedly starts.	2,48/yr It's assumed that initiating cause here is the operator (human action) making a mistake by pressing a button from the control room to start the HV PS when people are inside the PSS0 controlled area. Assuming that HV PS is turned on and off once per working day (see above) and conservatively assuming that a trained person makes mistake once every 100 operations, this gives the likelihood of 248/100 per year.	IN
IE03: A person affected by residual voltage upon entering the PSS0 controlled area.	The assumption here is that a person accesses the area twice per working day (496/year), but to be affected by residual voltage, the entry should be done within 250ms, which is not realistic and likelihood is chosen 0 (impossible to happen).	OUT Not credible event. Even without any additional protection, the capacitors and cable will discharge in 250ms through the 10MOhm resistors and it's not realistic to expect that somebody will enter the area in such short time.

There were some other events discussed during the HAZID meeting, but were not credited as initiating events for PSS0, for example:

- A person stands/working around ISrc and LEBT test stand area whilst the water is present on the floor (e.g. area flooded because of construction failure) and HV PS is on.
  - This event is not considered because the water needs to reach 1m of height (in 600m long and 6m wide tunnel) to make the area hazardous and there will be a procedure (included in the personnel training) not to go in the area or leave the area immediately in such case.
- A person got electrocuted inside PSS0 controlled area by touching the live parts intentionally or by mistake.
  - This event is not considered because all cable terminations and live parts will be protected with proper insulation material. The insulation prevents any access/accidental contact with live parts. It will be included in electrical safety training for personnel who will do the work in PSS0 controlled area.
- Fire fighters exposed to electrical hazard from HV PS upon entering the area to put out the fire.
  - PSS0 provides an emergency stop button outside the PSS0 area, which can be used to switch off HV PS. The main circuit board can also be used here as additional layer of protection. This event is not evaluated further in PSS0 hazard and risk analysis.

6.2. Barriers and procedures

6.2.1. Basic Process Control System for Ion Source

It is possible to switch-off the HV PS from the control room via the interlock PLC, which is connected directly to the HV PS interlock input (see [12] for more information). PSS0 will have the interface with this interlock PLC in parallel to PSS0 actuators to avoid hard switching-off the HV PS upon de-energising. It is also not possible to start the HV PS from the control room if the pre-defined sequence of pressing the “RESET” and “ON” buttons on the HV PS front panel (see [8]) is not detected by the interlock PLC, independently of PSS0. Since it’s a separate system from PSS0 and it doesn’t share any equipment with PSS0, it will be credited as Basic Process Control System (BPCS, see [1] for more information) in scenarios where a normal switch-off of the HV PS can remove the hazard with a probability of failure on demand (PFD) of 0,1.

6.2.2. Trapped key mechanical interlock key exchange

The PSS0 key exchange (see Figure 5) will be used for issuing the permit to power the HV PS and for accessing the PSS0 controlled area after removal of the electrical hazard, i.e. unlocking the access gate. Procedures for using the keys are described in [8], but an important part to mention here is a mechanical interlock of the PSS0 key exchange. Trapped key interlocking ensures that a process is followed and cannot be circumvented or shortcut. The transfer of a key ensures that wherever personnel find themselves, in

either starting or shutting down operations, they can be assured that they are safe. Mechanical interlock procedures are mentioned below.

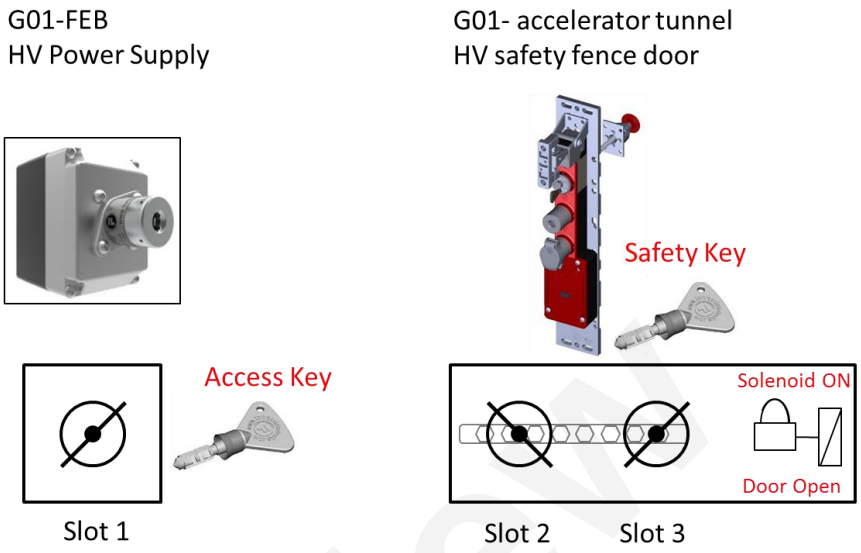


Figure 5: PSS0 key exchange.

- Accessing the PSS0 controlled area:
  - The Access key is used to start and stop the process (issue permit in case of PSS0) and upon removing this key from Slot 1 the hazard is isolated.
  - This key is then used to release Safety key from Slot 3, unlock the access gate and gain access to the PSS0 controlled area, but to be able to put Access key in Slot 2, the solenoid (electrical lock) shall be energised.
  - The Access key remains trapped in position while the Safety key is out of position and PSS0 area search status (see section below) is broken. In this way the Access key is trapped while access is gained and the HV PS cannot be started.
  - The access gate mechanical lock and Safety key are also mechanically interlocked, which means that Safety key cannot be returned into Slot 3 if the access gate is not closed.
- Ensuring there is no access whilst hazard is present:
  - To unlock the access gate and access the PSS0 area Safety key needs to be released as it serves as a safety token when somebody enters the area.
  - The Safety key is trapped in position while the Access key is out of position and PSS0 area cannot be accessed in this case.

6.2.3. Formalised search

The formalised search procedure is described in detail in [8]. The search status shall always be broken upon entering the PSS0 controlled area. Since the barriers and procedures definition considers that PSS safety functions are not in place, the importance here is on the procedure itself. It is assumed that before energising the HV PS there will be a person, i.e. an area supervisor, who would check the area to make sure nobody is

left inside and give permission to the operator to energise the HV PS. Since the PSS0 controlled area is very small (13,7m^2), it is conservatively assumed that human errors occur once per 100 years, giving the probability of failure without any PSS0 devices (e.g. light and sounders) of 0,01.

6.2.4. Grounding rod placement procedure

To satisfy requirements from Swedish standards for electrical safety [13], the grounding relay is used to ensure that the stored energy from the power supply and its output cable dissipates completely to the earth. The grounding rod is used in parallel as a nice-to-have addition for the same purpose (see Section 2.2. in [8]), but depends on human action and is not used for ensuring any of the safety functions. It is also not realistic to expect personnel to move extremely fast (less than 250ms) from the HV PS to the PSS0 controlled area gate and place the grounding rod in rush. Since this procedure does not have a real effect on the development of hazardous scenarios, it will not be considered in the hazard and risk analysis for PSS0.

6.3. Safety functions

Table 5 provides the high-level description of safety instrumented functions (SIFs) identified in the hazard register. A more detailed safety functions assessment covering the Safety Integrity Level (SIL) determination and verification will be done in IEC 61508 Overall Safety requirements and their allocation document [5].

Table 5: PSS0 SIFs.

SIF ID	SIF	Description
SIF01	High Voltage Power Supply emergency stop	Switch-off high voltage power supply upon pressing the emergency stop button.
SIF02	HV interlock upon intrusion to PSS0 controlled area	Switch-off high voltage power supply upon detecting the intrusion (access gate in open position).
SIF03	HV interlock – PSS0 key exchange	Switch-off HV PS upon removing the Access key from Slot 1 and ensure the HV platform is grounded. Ensure that HV cannot be started if Safety key is not in place.
SIF04	Door lock – PSS0 key exchange	Prevent access by activating the access gate lock upon removing Access key from Slot 2.
SIF05	HV ON warning light	Alert personnel around PSS0 controlled area that HV PS is on by activation HV ON warning light and additionally, activate area blue light in LEBT area.

Note: 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 so it will be in the list of SIFs, but will be treated as part of administrative control in the analysis.

6.3.1. PSS0 interfaces

The main interface for implementing PSS0 SIFs is with the ISrc HV PS. This interface between PSS0 PLCs and HV PS is described in detail in the Accelerator Personnel Safety System 0 and Ion Source Interface Control Document [12]. To ensure functionality of interlock (switching off) safety functions, PSS0 will de-energise two contactors (redundancy to avoid single failure), which are interrupting the mains incoming power to the HV PS.

6.4. Analysis of initiating events – accident progression

6.4.1. Event Tree Analysis

The hazardous scenario progression leading to a consequence is logically presented using the Event Tree Analysis (ETA) method. In this document the qualitative ETA is performed, which will be used for assessment of safety functions in [5]. The ETA methodology is described in Figure 6.

6.4.2. PSS0 Conventional Safety consequences

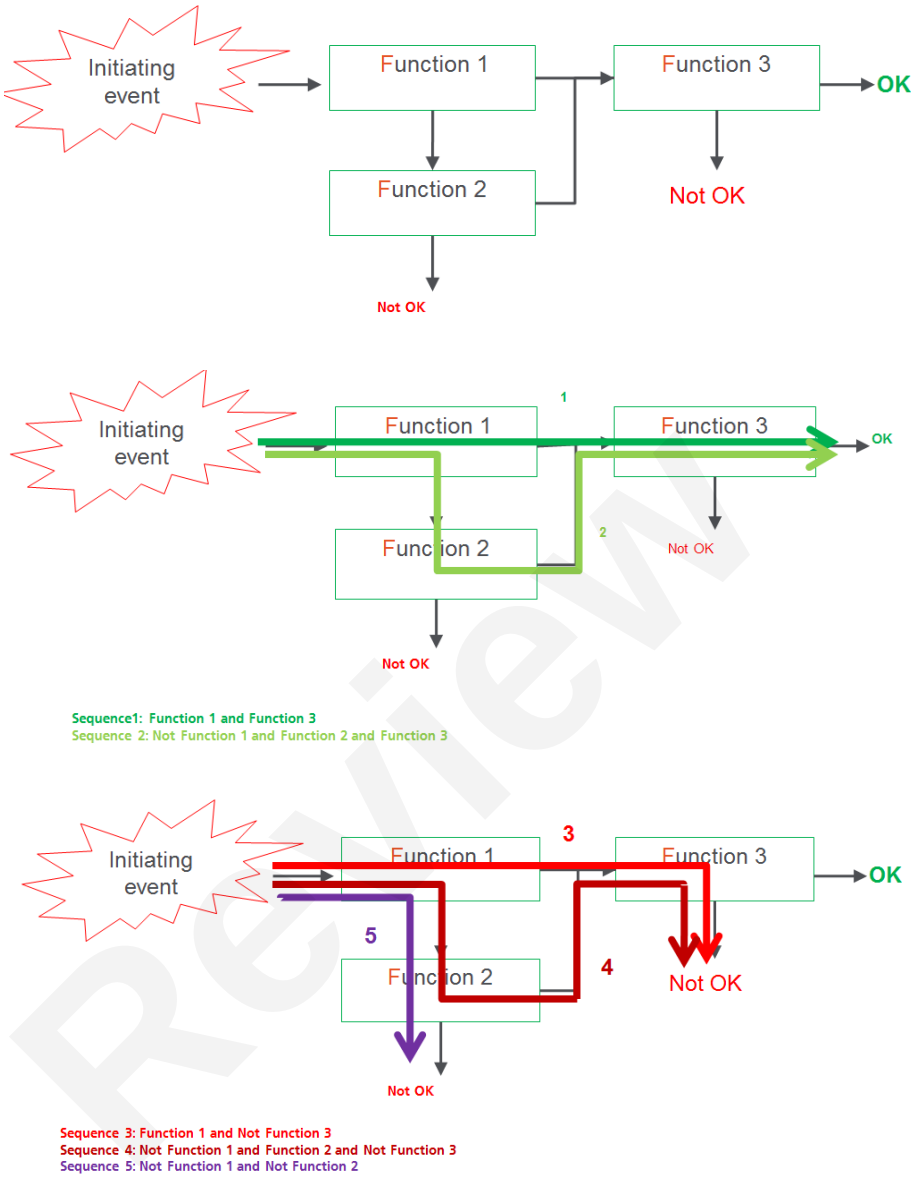
Table 6 shows the conventional safety consequences for PSS0 defined in [3], which are used in Conventional Safety Risk Matrix shown in Table 7.

Table 6: PSS0 Conventional Consequences.

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

Table 7: Conventional Safety Matrix for PSS0.

			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	5	$<10^{-6}$	5A	5B	5C	5D	5E



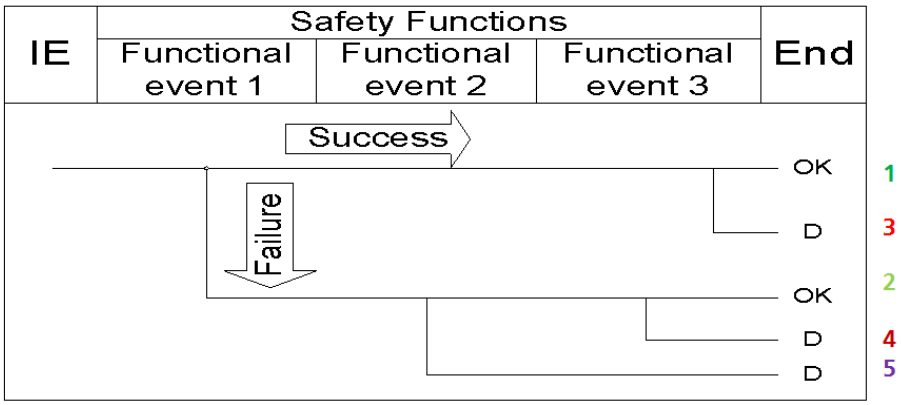


Figure 6: Event Tree Analysis method.

Considering the assumption listed in Section 4.2 - if a person enters the PSS0 controlled area when the HV PS is powered it is considered fatal, and to simplify the safety analysis, only two safety consequences are credible for PSS0:

- No safety consequences – equivalent to Negligible in Table 6.
  - Hazard avoided by successful procedure, alarm or PSS0 SIF.
  - PSS0 controlled area is safe, HV PS is switched off.
- Electric shock, fatality – equivalent to Hazardous in Table 6.
  - Failure of procedures, alarms and/or PSS0 SIF.
  - PSS0 controlled area is hazardous, HV PS is switched on.

6.4.3. PSS0 initiating events Event Tree Analysis

An ETA for PSS0 was carried out using Isograph Reliability Workbench v13 software (incorporating FaultTree+). The results are shown in Figures 7-9 below:

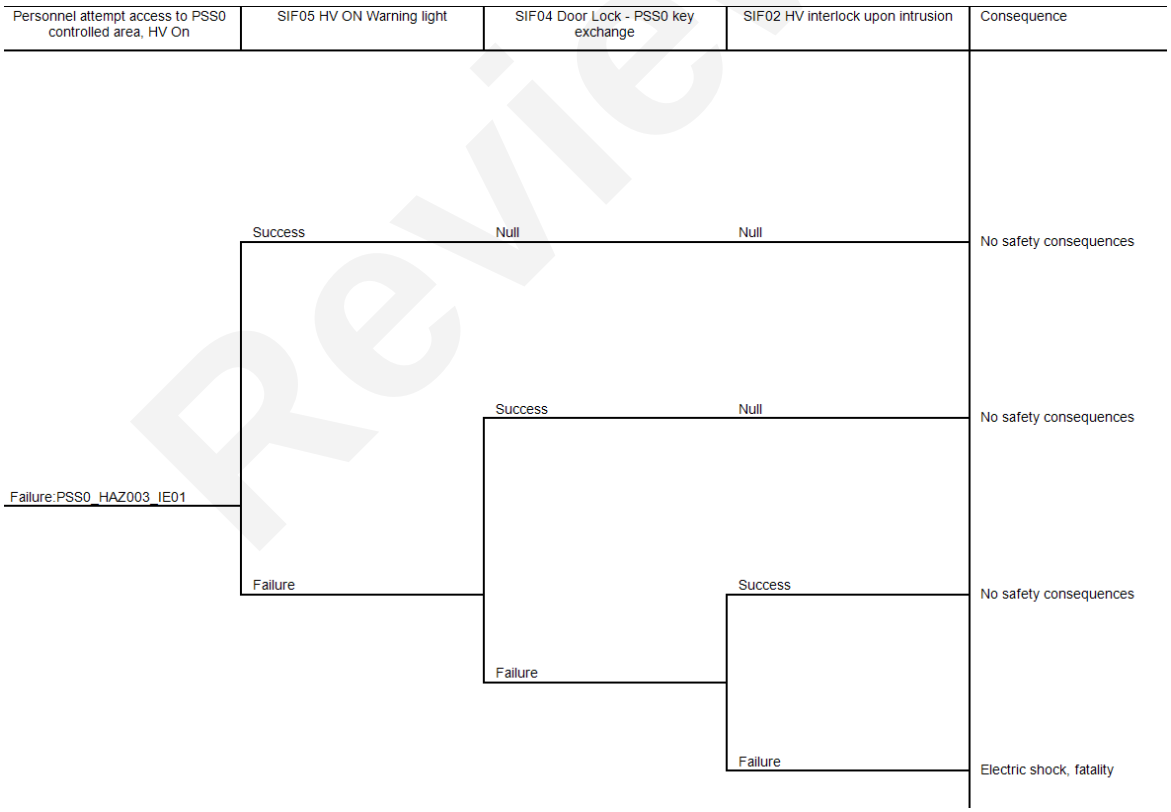


Figure 7: ETA for initiating event 01.

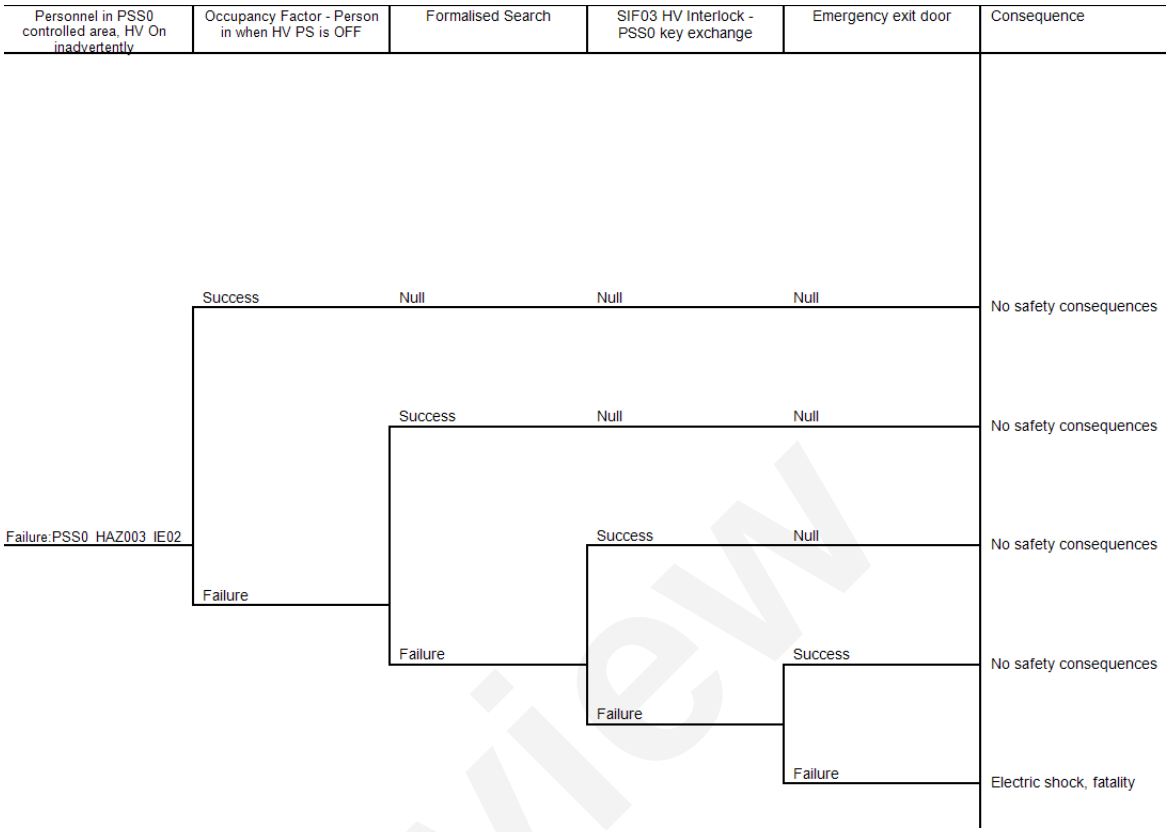


Figure 8: ETA for initiating event 02.

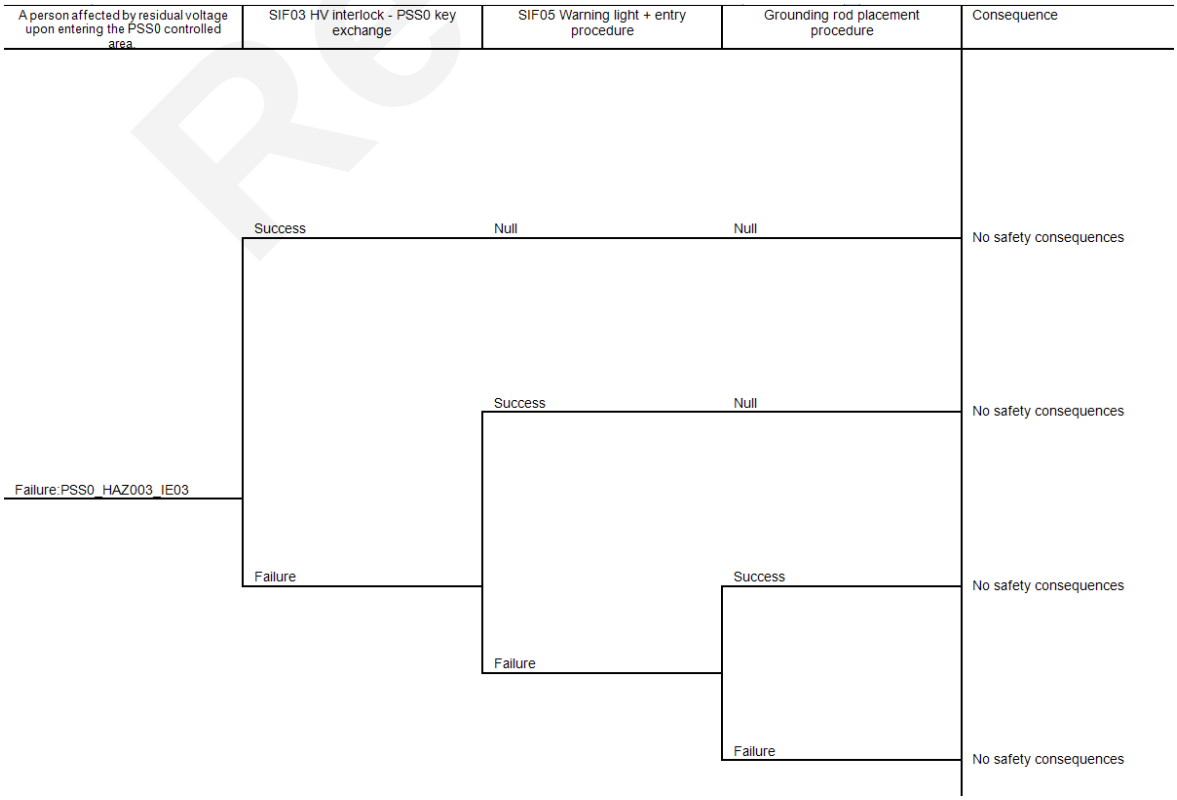


Figure 9: ETA for initiating event 03.

7. CONCLUSION

The risk is a product of the magnitude of potential consequence and likelihood (probability) of this consequence to occur. The qualitative hazard and risk analysis performed for PSS0 shows the need for safety instrumented functions to lower the probability of occurrence of the worst case scenarios. In this case it is a fatality caused by electric shock. A list of needed safety functions and ETA failure scenarios are provided in this document and will be used in the IEC61508 Overall Safety Requirements and their Allocation Document for PSS0 [5], to carry out quantitative analysis (using 10^{-6} per year as a broadly accepted tolerable risk level), determination and verification of safety integrity levels.

8. REFERENCES

[1] IEC61508:2010. Functional Safety of electrical/ electronic/ programmable electronic safety-related systems.

[2] IEC 61511:2016. Functional safety - Safety instrumented systems for the process industry sector.

[3] ESS-0217911: IEC 61508 Concept Document for the Accelerator Personnel Safety System 0.

[4] ESS-0237881: IEC 61508 Scope Document for the Accelerator Personnel Safety System 0 (PSS0).

[5] ESS-0231390: IEC61508 Overall Safety Requirements and their Allocation Document for PSS0.

[6] Morteza Mansouri: Visit to INFN- Catania (2017-07-17 till 2017-07-19), https://confluence.esss.lu.se/pages/viewpage.action?pageId=227674094.

[7] ESS-0122281: Ion source high voltage protection cage.

[8] ESS-0134492: Concept of Operations for the Accelerator Personnel Safety System 0 (PSS0).

[9] Øystein Midttun: 2017-11-01 Ion Source safety cage and PSS0 design review, https://confluence.esss.lu.se/display/LG/2017-11-01+Ion+Source+safety+cage+and+PSS0+design+review.

[10] ESS-0236105: PSS0 Official HAZID Meeting Minutes

[11] ESS-0229491: PSS0 Hazard register

[12] ESS-0237562: Accelerator Personnel Safety System 0 and Ion Source Interface Control Document

[13] SS-EN 50110-1:2013. Skötsel av elektriska anläggningar – Del 1: Allmänna fordringar; *Operation of electrical installations – Part 1: General requirements*

9. DOCUMENT REVISION HISTORY

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