|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Concept of Operations For the Accelerator Personnel Safety System 0 (PSS0) |
|  |
|  |

|  | Name | **Role/Title** |
| --- | --- | --- |
| **Author** | Morteza Mansouri | Lead Integrator Engineer for Safety Critical Systems, ICS Division |
| **Owner** | Stuart Birch | Senior Engineer, Personnel Safety Systems, ICS Division |
| **Reviewer** | Jörgen Mattsson  Edgar Sargsyan  Meike Rönn | Senior Electrical Safety Engineer, ES&H Division  Section Leader Front End & Magnets, AD  Technical Documentation Specialist, ICS |
| **Approver** | Peter Jacobsson  Annika Nordt | Head of Environment, Safety & Health Division  Group Leader for Protection Systems Group, ICS |
| **Distribution List** | Alejandro Garcia Sosa  Lali Tchelidze  Marcos Munoz  Lena Johansson  Michael Plagge  Helen Boyer  Denis Paulic  Yong Kian Sin | Ion Source Scientist, Front End & Magnets Section  Section Leader for Operations, AD  Senior Scientist, Operations Section, AD  Senior Radiation Protection Expert, ES&H Division  Occupational Health & Safety Engineer, ES&H Division  Group Leader for Occupational Health & Safety Group, ES&H Division  Deputy Group Leader for Protection Systems Group, ICS  Electrical Controls Engineer, ICS Division |

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

1. Introduction 4

1.1. Purpose 4

2. System characteristics 5

2.1. System purpose 5

2.2. System overview 5

2.2.1. Components 5

PSS0 is an electrical safety interlock system consisting of the following equipment: 5

2.2.2. PSS0 architecture 6

2.2.3. Supervision 6

3. System Stakeholders, roles and responsibilities 7

3.1. ICS 7

3.2. AD 7

3.3. ES&H 7

4. Concepts of operations 8

4.1. Environment 8

4.2. Barriers and procedures 9

4.2.1. Basic Process Control System for Ion Source 9

4.2.2. Trapped key mechanical interlock key exchange 9

4.2.3. Formalised search 10

4.2.4. Grounding rod placement procedure 10

4.2.5. HV ON and Beam ON warning lights 10

4.3. Operating scenarios 11

4.3.1. Energising HV PS 11

4.3.2. De-energising the HV PS and access to PSS0 controlled area during normal operation 12

4.3.3. De-energising the HV PS and access to ISrc fenced area in case of emergency 12

4.3.4. Maintenance in ISrc HV platform 13

4.4. Maintenance 13

5. References 14

6. Definitions, acronyms and abbreviations 15

Document Revision history 16

# Introduction

## Purpose

The purpose of this document is to describe the concepts of operations for Accelerator Personnel Safety System 0 (PSS0). This document gives a description of the initial design of the Personnel Safety System to be installed for the ESS accelerator Ion Source (ISrc) and Low energy beam transport (LEBT) test stand. It also provides instructions for PSS0 operating procedures. Requirements on the initial design are given by the overall safety requirements in [7]. Hazards to be mitigated and relevant initiating events from [8] and [7] are also taken into consideration for the initial design.

# System characteristics

This chapter describes the initial design of the Personnel Safety System 0 (PSS0) to be installed for the IScr and LEBT.

## System purpose

As described in [7], PSS0 aims to mitigate high voltage electrical hazards for personnel arising from operating the ISrc and LEBT test stand.

The PSS0 design is chosen to meet the requirements in SS-4364000 which is a Swedish standard for Low-voltage electrical installations - Rules for design and erection of electrical installations[1].

The system operation is chosen to meet the requirements in SS-EN 50110-1:2013, a European standard for operation of electrical installations [2]. It should be noted that, in the context of this document “operation” means all activities including work activities necessary to permit the electrical installation of the ISrc HV PS to function.

## System overview

### Components

### PSS0 is an electrical safety interlock system consisting of the following equipment:

* Two independent safety position monitoring switches (magnetic safety switch and mechanical safety switch) to monitor the positon (i.e. open or closed) of the PSS0 controlled area access door.
* The PSS racks containing the PSS0 red and blue train CPUs, PSS0 remote I/Os, and PSS0 contactors for the ISrc HV PS, which are installed in FEB level 90.
* Two contactors (in series) on mains incoming power to ISrc HV PS in order to disconnect the HV PS from energy source completely, upon access to PSS0 controlled area.
* A safety fence around the ISrc HV platform (provided by AD), which functions as a barrier against direct contact to the ISrc HV platform and prevents any access to PSS0 controlled area during operation of the ISrc. Before the ISrc HV platform can be energised by the HV PS, the PSS0 controlled area has to undergo a formalised search ensuring no worker is inside PSS0 controlled area. In addition, to finish search, the access door to PSS0 controlled area must be locked.
* HV grounding relay and grounding rod to carry out earthing and short-circuiting of ISrc HV PS output. It should be noted that the HV grounding relay has the main function to ensure grounding of the ISrc HV platform, and the grounding rod will be used as an additional layer of protection.
* Key exchange system and door lock (amGard pro Fortress proLok) to provide a predefined mechanical sequence to de-energise the HV PS and provide access to PSS0 controlled area.
* Search buttons to be used to carry out a formalised search in PSS0 controlled area prior to energising the ISrc HV PS.
* Emergency stop button to be installed outside PSS0 controlled area, and in the vicinity of the ISrc and LEBT test stand.

Appendix 1 details a plan view of accelerator tunnel and klystron gallery, highlighting the areas where LCR, PSS0 controlled area and PSS0 racks are situated.

Appendix 2 details the distribution of PSS0 field devices in FEB level 90 and PSS0 controlled area.

Appendix 3 details an overview of PSS0 interfaces with ISrc. The details of Interfaces between PSS0 and ISrc are described in [3].

### PSS0 architecture

PSS0 is built using two identical Siemens PLC and distributed I/O system with redundant sensors and actuators. This is also known as “two train system”; distinguished as “red train” and “blue train”.

Appendix 9 details the network architecture of PSS0.

### Supervision

The GUI for PSS0 monitoring will be developed as below:

* In LCR:

The status of PSS0 will be shown in LCR as below.

* + PSS0 OK/NOK
  + PSS0 Permit to ISrc HV PS Enabled/Disabled

These two signals are available in the ISrc GUI (which is developed using CSS as the container for EPICS clients GUIs) in LCR. The PSS0 status is sent via hard-wired signals to interlock PLC (the PLC for ISrc and LEBT control system), which is communicating with EPICS and CSS in LCR. It should be noted that these signals are read only.

* In FEB:

There will be an HMI for each of PLC trains installed on the PSS0 racks in FEB.

The HMIs will provide the details of PSS0 status, such as PSS0 mode, diagnostics signals, etc. The PSS0 reset can be done through these HMIs as well. The HMIs are password protected, and can be accessed only by PSS personnel.

# System Stakeholders, roles and responsibilities

This chapter details the responsibilities of relevant stakeholders in regards to PSS0 development.

## ICS

The protection systems group in ICS is responsible to develop, install, commission, validate and maintain PSS0.

## AD

AD is responsible to develop, install and maintain the ISrc safety fence, and operate the PSS0 system according to all the procedures described in this document. The operations personnel roles and responsibilities for the ISrc and LEBT test stand are described in [6].

## ES&H

ES&H is responsible to provide ICS with overall requirements on safety functions to be implemented by the PSS0, approve the conformity of PSS0 operation and design with applicable rules and guidelines at ESS.

# Concepts of operations

This chapter gives an overview over intended operation of the PSS0. First, the ISrc and LEBT are explained briefly, then barriers and procedures to be installed for PSS0 and intended operating scenarios are given.

## Environment

PSS0 will be installed to mitigate electrical hazards for personnel arising from operating the ISrc and LEBT test stand. The ISrc and LEBT will be installed in Accelerator tunnel. Figure 1 shows a 3D model of the ion source and LEBT. The ISrc and the racks for control systems I/Os, vacuum, etc. are situated inside a metallic cage, which is called the ISrc HV platform. There are 9 steel doors for the ISrc HV platform. The high voltage platform houses the plasma chamber as well as the controls and power supplies needed for plasma generation. The platform is biased to 75 kV DC to allow extracting of a 75 keV proton beam. The LEBT consist mainly of two solenoids to focus the beam, an iris to reduce the beam current, a chopper to remove the first part of the beam, and diagnostics [4].

It shall be noted that the HV PS maximum output power rating is 100 kV and 150 mA, DC.

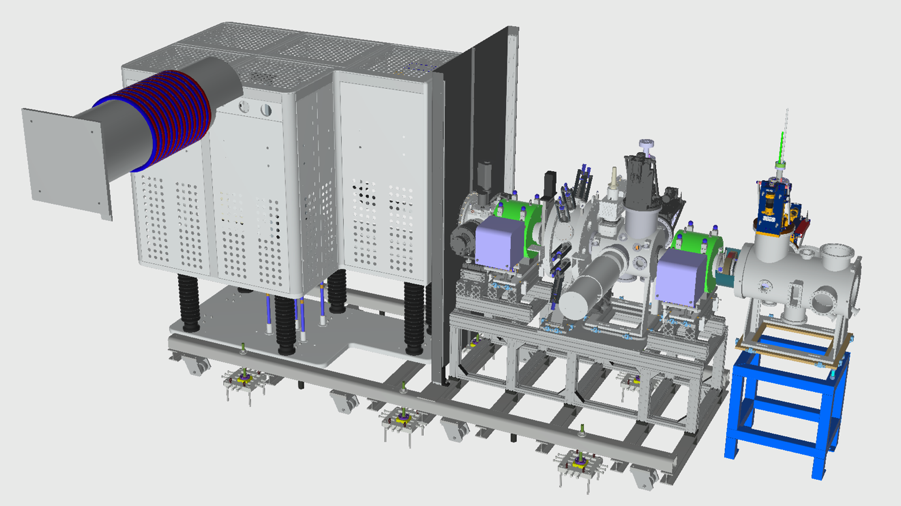


Figure 1: Ion source high voltage platform (left), and LEBT (right).

The ISrc HV platform will be surrounded by a fence to provide protection against direct contact to ISrc HV platform when the HV PS is energised. The fence design conforms to IP 3X and its detailed design is described in [5].

The HV PS is installed in FEB level 090 and the HV cable runs through a dedicated cable route to the ISrc HV platform.

## Barriers and procedures

This section presents the concept for designing the barriers and procedures.

### Basic Process Control System for Ion Source

It is possible to switch off the HV PS from the control room via a programmable logic controller (PLC), imposing an interlock on the equipment. This PLC is connected directly to the HV PS interlock input. For the BPCS to energize the HV PS, the PSS0 interlock shall be enabled. Since the BPCS is a separate system from PSS0 and it does not share any equipment with PSS0, it will be credited as Basic Process Control System (BPCS, see [10]) for more information) in scenarios where a normal switch-off of the HV PS can remove the hazard.

### Trapped key mechanical interlock key exchange

The PSS0 key exchange (see Figure 3) will be used for issuing the permit to power on the HV PS and for accessing the PSS0 controlled area after removal of the electrical hazard, i.e. unlocking the access door. Details on procedures for using the keys are described in Appendix 6. An important part to discuss 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 when accessing the PSS0 controlled area. 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.

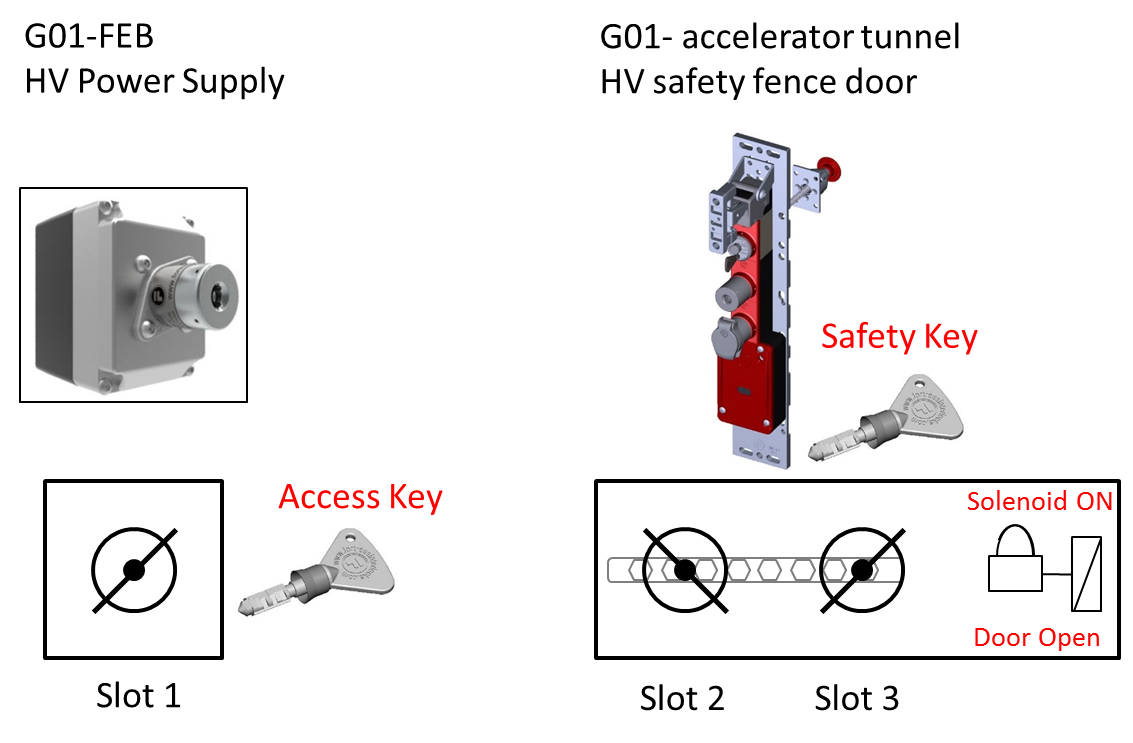


Figure 3: PSS0 key exchange.

* 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 put in Slot 2 to release Safety key from Slot 3, unlock the access gate and gain access to the PSS0 controlled area. To be able to put Access key in Slot 2, the solenoid (electro-magnetic lock) shall be energised.
      * The Access key remains trapped in position while the Safety key is out of position and the 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.

### Formalised search

The formalised search procedure is described in detail in Appendix 4. 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 nominated person, 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 (13,7m2), 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.

### Grounding rod placement procedure

To satisfy requirements from the Swedish standards for electrical safety [1], a grounding relay is used to ensure that the stored energy from the power supply and its output cable dissipates completely to the earth. A grounding rod is used in parallel as a back-up possibility for the same purpose. However, it depends on human action and is not primarily used for ensuring any of the safety functions. Since this grounding rod placement procedure does not have a real effect on the development of any hazardous scenarios as listed above, it will not be considered in the hazard and risk analysis for PSS0.

### HV ON and Beam ON warning lights

The PSS team will install three warning lights around the PSS0 controlled area: the red “HV ON” and blue “Beam ON” warning lights near the access door, outside the PSS0 controlled area, and additional blue “Beam ON” light in the LEBT area. They will be used to alert present personnel that the HV PS is on and the PSS0 controlled area is hazardous. The logic for activation of these lights will be implemented through standard part of the PSS0 software and is conservatively estimated to fail once per ten requests, resulting in a PFD of 0.1.

## Operating scenarios

The operating scenarios described below will be carried out by the Shift Leader and Operator(s) whose roles and responsibilities are defined in [6].

### Energising HV PS

In order to enable ISrc operation, the HV PS needs to be energised.

Following the issue of ISrc operation permit by Shift Leader, the operator shall carry out all the procedures mentioned below step by step to energise the HV PS.

Prior to energising of ISrc HV PS, the operator shall ensure that there is no one inside PSS0 controlled area. This will be done through formalised search. Appendix 4 details the procedures to carry out formalised search in PSS0 controlled area.

In appendix 4:

* Steps 1 to 9:

The operator makes sure there is nobody inside the HV platform, and all the 9 steel doors of the ISrc HV platform are closed.

* Step 10:

The operator looks around the area within the PSS0 controlled area to ensure there is no one present there, and presses search button #1.

* Step 11:

The operator walks towards search button #2, and looks around the area within the PSS0 controlled area to ensure there is no one present there, and presses search button #2.

* Step 12:

The operator removes the grounding rod from the ISrc HV platform, and will place the grounding rod in its rest place next to the PSS0 controlled area access door. (The position of the grounding rod in its rest place is being monitored by the mechanical micro-switches of the grounding rod)

* Step 13:

The operator leaves the PSS0 controlled area and closes the door.

In the highly improbable event that a person is left inside PSS0 controlled area during the formalised search, the person (upon hearing the search sounder tone) can unlock the access door and exit the PSS0 controlled area by pressing the escape release button which is installed next to the access door. As soon as the access door is open, the safety position monitoring switches installed on the access door will trip the ISrc HV PS mains incoming power.

Appendix 5 details a flowchart for sequences of actions to energise the ISrc HV PS.

Appendix 6 details PSS0 key exchange philosophy during energising ISrc HV PS.

### De-energising the HV PS and access to PSS0 controlled area during normal operation

In order to access PSS0 controlled area, the HV PS shall be de-energised. Following the issue of permit to access PSS0 controlled area by the Shift Leader, the operator shall carry out the procedures mentioned below step by step to de-energise the HV PS, and get access to PSS0 controlled area.

Appendix 7 details flowchart for sequences of actions to de-energise the ISrc HV PS, and access to PSS0 controlled area.

Appendix 6 details PSS0 key exchange philosophy during de-energising ISrc HV PS, and access to PSS0 controlled area.

### De-energising the HV PS and access to ISrc fenced area in case of emergency

* In case of emergency (e.g. fire or risk of explosion in the ISrc and LEBT test stand area), an emergency stop button is installed outside PSS0 controlled area, in the vicinity of the ISrc and LEBT test stand [see appendix 2]. The main objective of this emergency stop button is to provide means for quick intervention of operator(s) to de-energise the ISrc HV PS in the event of an incident that could jeopardize the integrity of the Ion Source.
* The Fortress lock on the access door to PSS0 controlled area need to be energised to unlock the door (in addition to the presence of the Access key). In case of solenoid failure, the access to PSS0 controlled area can be granted using a mechanical override key for the Fortress lock. The Shift Leader, who is in charge of ISrc and LEBT test stand operation, is in possession of the mechanical override key, to unlock the access door from outside. This override key shall only be used in case of emergency when quick access to PSS0 controlled area is required. It should be noted that as soon as the access door is open, the safety position monitoring switches installed on the access door will trip the ISrc HV PS mains incoming power.

Appendix 8 details flowchart for sequences of actions to de-energise the ISrc HV PS, and access to PSS0 controlled area in case of emergency.

### Maintenance in ISrc HV platform

During access to PSS0 controlled area, the distribution board and equipment on the ISrc HV platform are still energised (400 VAC). This can expose personnel (who are carrying out maintenance of equipment on ISrc HV platform) to electrical hazards. Therefore, appropriate measures such as Lockout Tag-out of electrical equipment on ISrc HV platform shall be carried out by the operator(s) prior to maintenance activities.

## Maintenance

In addition to preventive and corrective maintenance on PSS0, proof tests will be performed as well.

Any maintenance or repair (if required) for PSS0 will be carried out during ISrc and LEBT shutdown.

# References

1. SS 4364000 Swedish standard; Low-voltage electrical installations - Rules for design and erection of electrical installations
2. SS-EN 50110-1:2013 European standard; Operation of electrical installations – Part 1: General requirements
3. Accelerator Personnel Safety System 0 and Ion Source Interface Control Document (ESS-0237562)
4. Technical Description of the ESS Normal Conducting Front End (ESS-0159957)
5. Ion Source Safety Fence (ESS-0122281)
6. Operations Personnel Roles and Responsibilities in the ESS Main Control Room (ESS-0149550)
7. Overall safety requirements and initiating events analysis (ESS-0229506)
8. Hazards and risk assessment of the ion source and LEBT (ESS-0118213)
9. PSS0 Hazard register (ESS-0229491)
10. SIL Assessment Report (ESS-0231390)

# Definitions, acronyms and abbreviations

**Abbreviation Explanation of the abbreviation**

AD Accelerator Division

CSS Control System Studio

EPICS Experimental Physics and Industrial Control System

ES&H Environment, Safety & Health Division

ESS European Spallation Source

FEB Front End Building

GUI Graphical User Interface

HMI Human Machine Interface

HV PS High Voltage Power Supply

ICS Integrated Control System Division

ISrc Ion Source

LCR Local Control Room

LEBT Low Energy Beam Transport

PSS Personnel Safety System

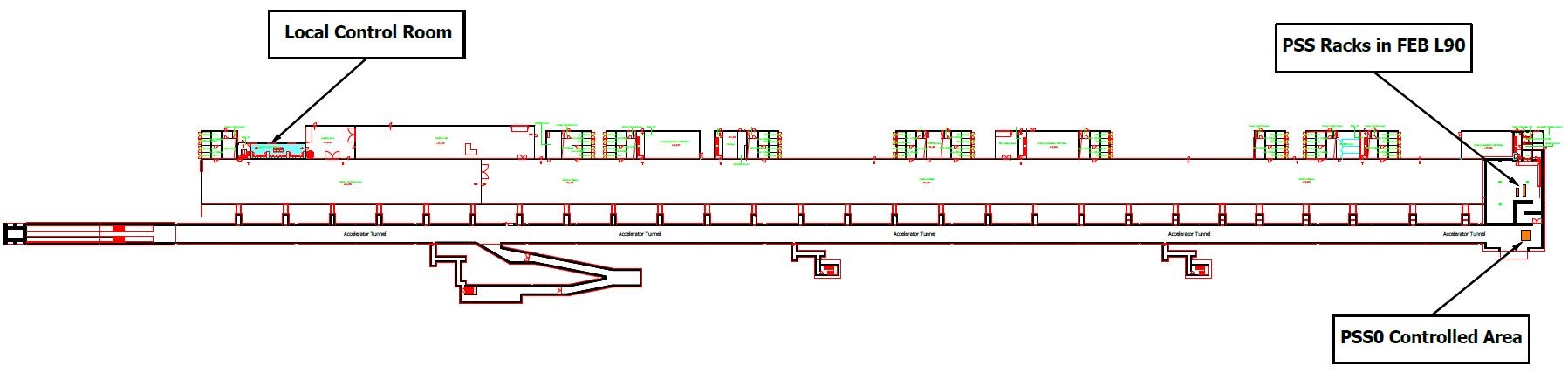
PSS0 Personnel Safety System for ISrc and LEBT Test Stand

Z0 Zone0: PSS0 Controlled Area

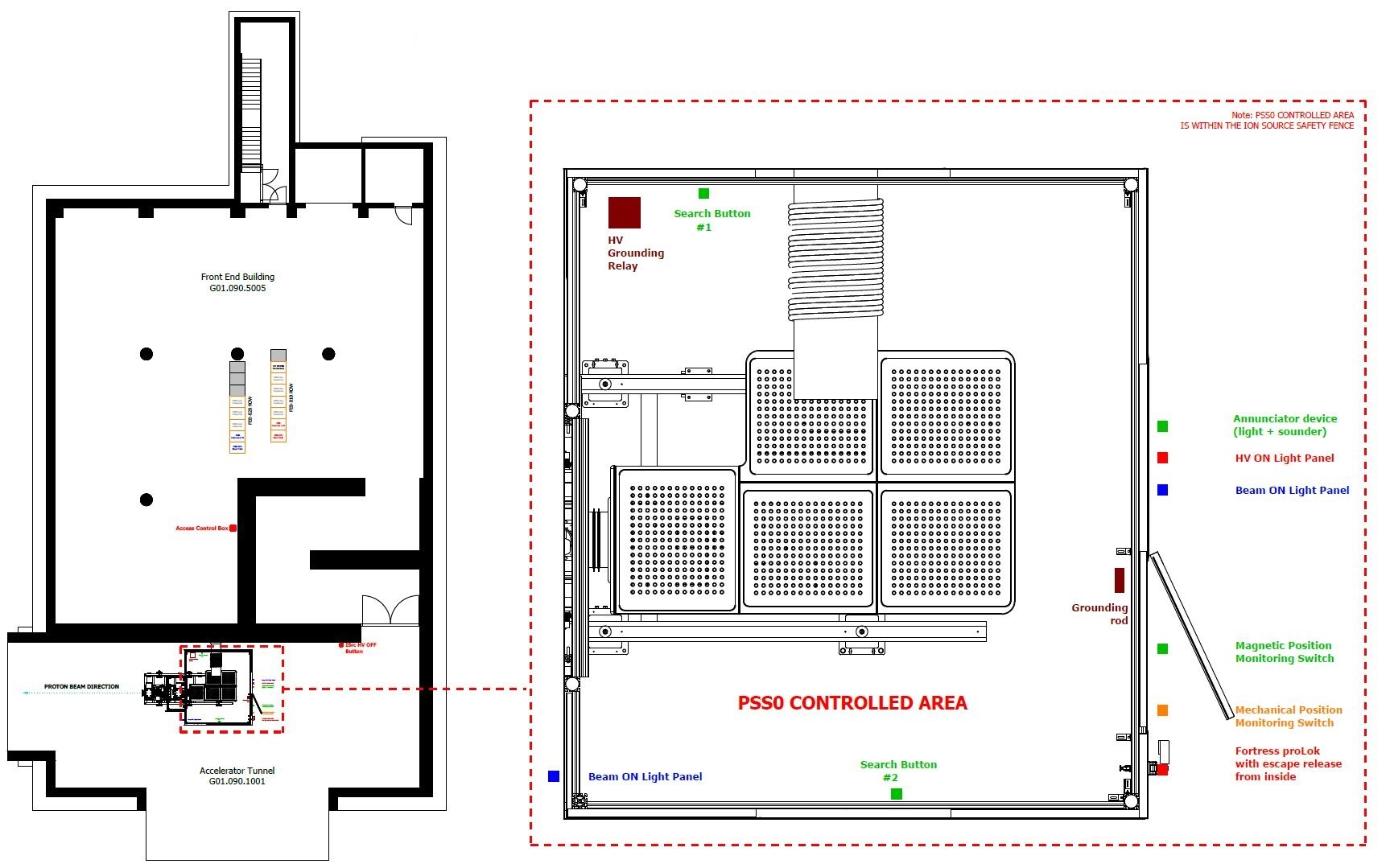
Document Revision history

| Revision | Reason for and description of change | Author | Date |
| --- | --- | --- | --- |
| 1 | First issue | Morteza Mansouri | 2017-10-13 |
| 2 | Implemented the recommendations from PSS0 CDR (ESS-0268277)  Re-structured the document by removing the flowcharts from the text and adding them as appendices.  Added formalised search and key exchange philosophy in appendices.  Added reference to Operations Personnel Roles and Responsibilities (ESS-0149550)  Added a chapters about PSS0 architecture and supervision. | Morteza Mansouri | 2018-04-19 |
|  |  |  |  |

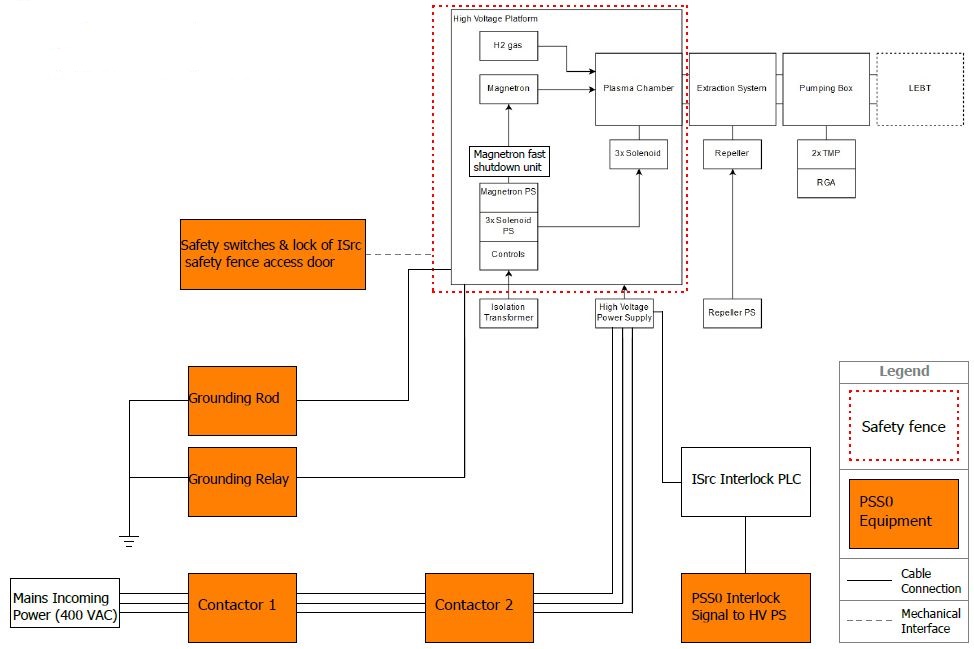
**Appendix 1: PSS0 Controlled Area and LCR Location in Accelerator Buildings**



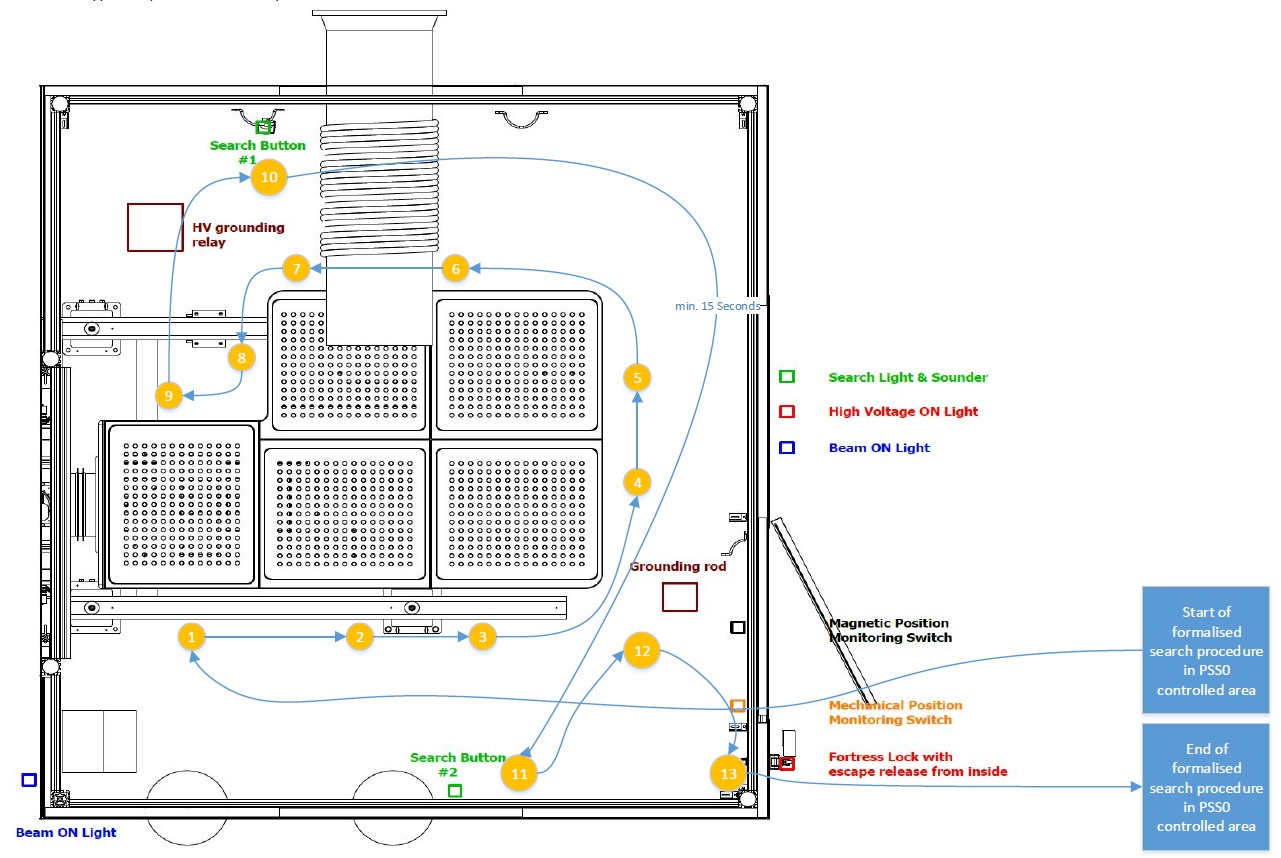
**Appendix 2: PSS0 Equipment Distribution**



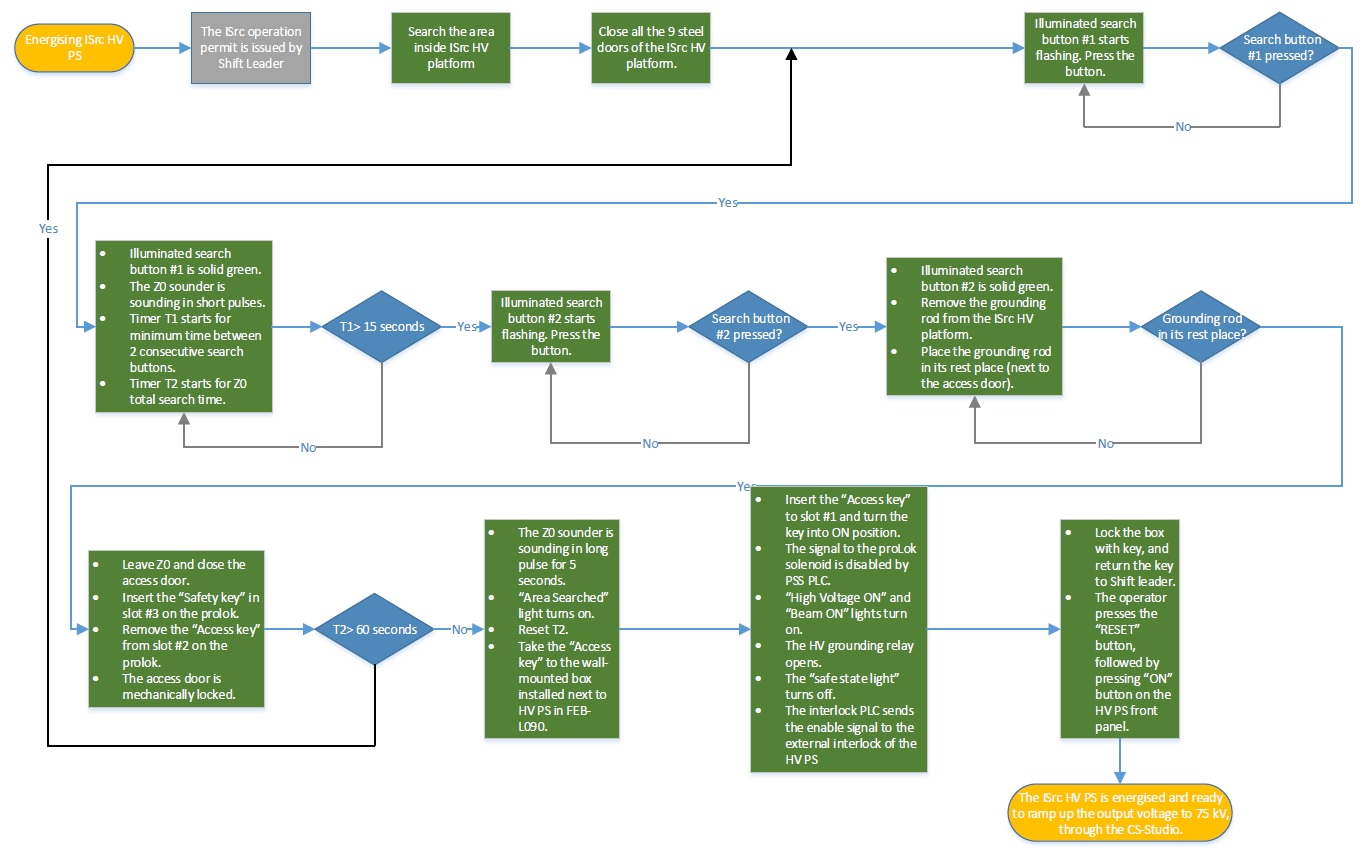
**Appendix 3: PSS0 Interfaces with ISrc**



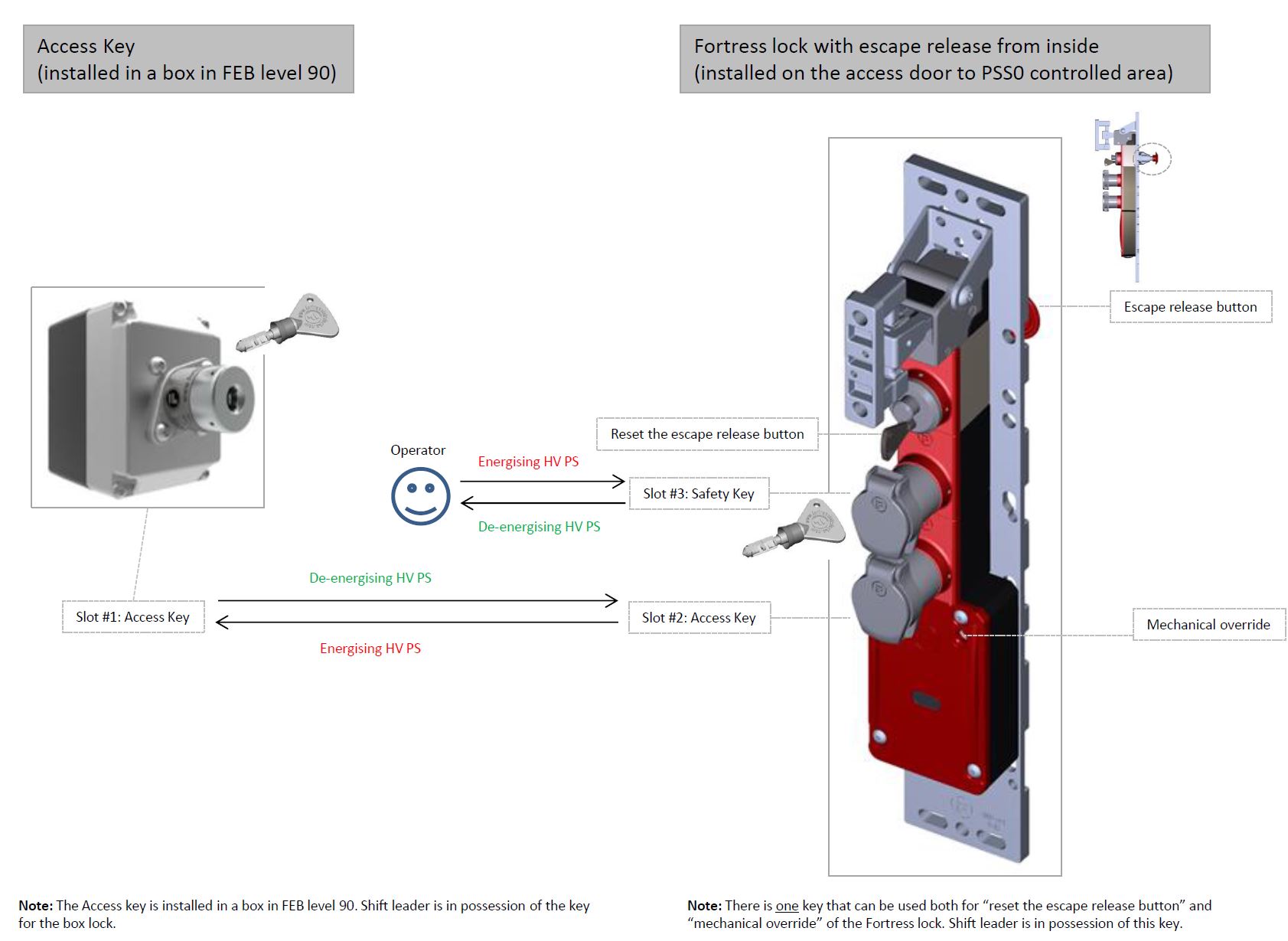
**Appendix 4: PSS0 Formalised Search**



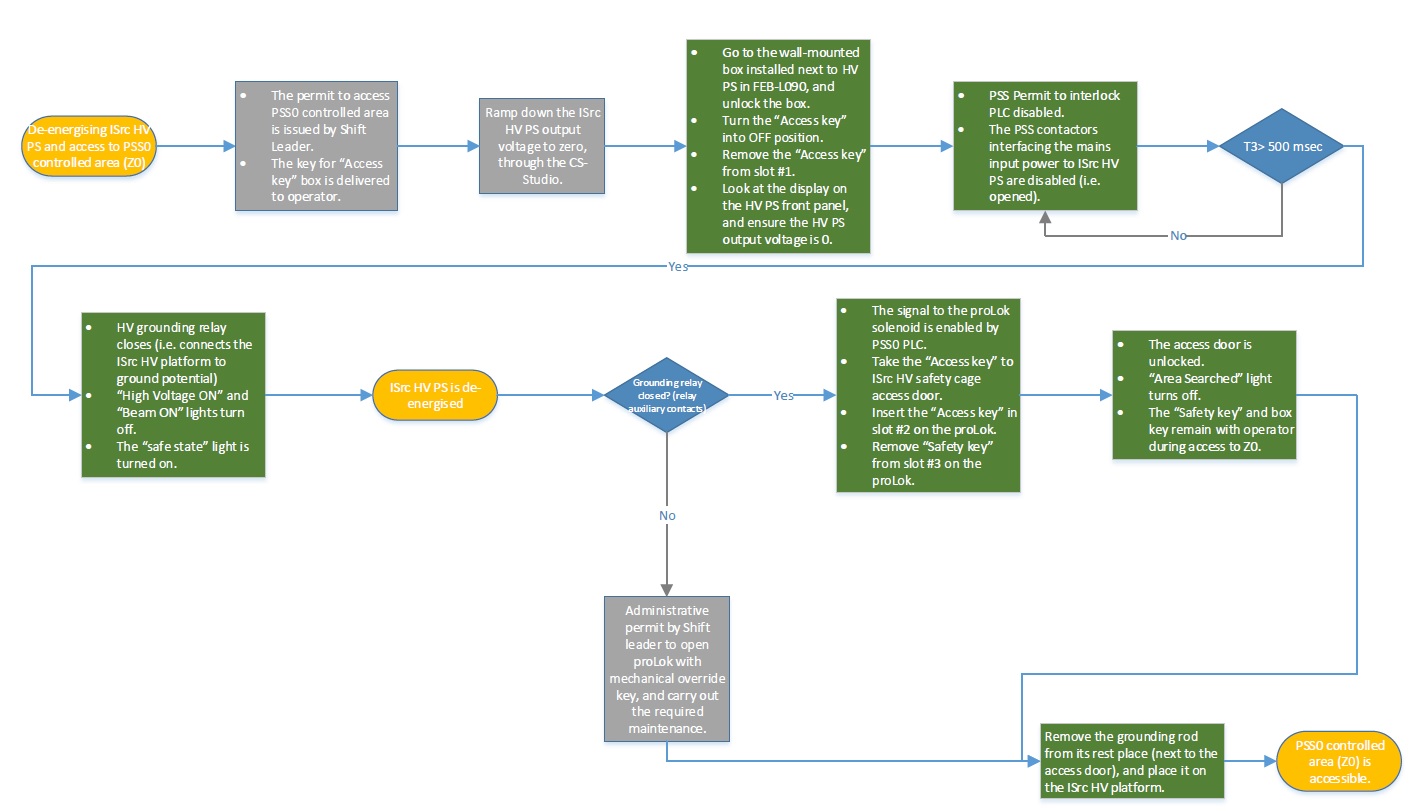
**Appendix 5: PSS0 Energising ISrc HV PS**



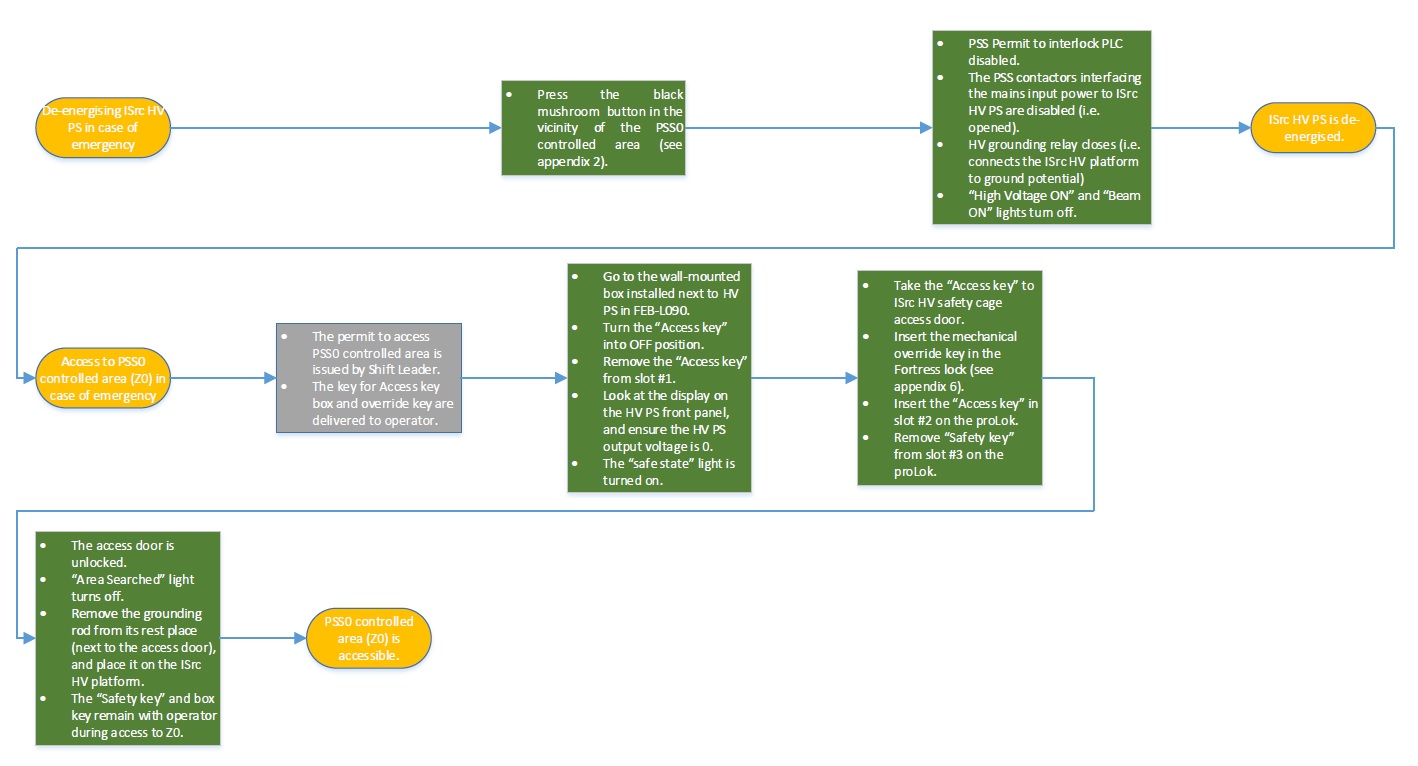
**Appendix 6: PSS0 Key Exchange Philosophy**



**Appendix 7: PSS0 De-energising ISrc HV PS**



**Appendix 8: PSS0 De-energising ISrc HV PS in Emergency**



**Appendix 9: PSS0 Architecture**

