Jefferson Lab Personnel Safety Systems

Systems Requirement Specification

Version 2.1

May 21, 2007

Table of Contents

1 Introduction 1

1.1 Safety Systems 1

2 Scope 2

3 Mission of the PSS 3

4 Design Basis 3

5 References & Standards 4

5.1 ANSI (American National Standards Institute) 4
5.2 IEC (International Electro-technical Commission) 4
5.3 U.S. Department of Energy Orders 4
5.4 U.S. Code of Federal Regulations 4
5.5 National Council on Radiation Protection (NCRP) 4
5.6 International Atomic Energy Agency (IAEA) 4
5.7 National Fire Protection Association (NFPA) 5
5.8 International Society for Automation (ISA) 5
5.9 Jefferson Laboratory requirements, Standards, and Guidelines 5
5.10 Jefferson Lab Reports and Notes 5

6 Safety Assessment Document (SAD) Requirements 6

6.1 Operations and Safety Envelope 6
6.2 Certification and Test 6
6.3 Staffing 6
6.4 Fault Tolerance 6

7 Safety Functions 7

7.1 SF1 Prevent Beam Transport to Occupied Areas 8
7.2 SF2 Shut off interlocked devices when physical barriers are unsecured. 9
7.3 SF3 Shut off interlocked devices upon activation of an ESTOP 9
7.4 SF4 Inhibit operation of interlocked devices in support of secure administrative access. 9
7.5 SF5 Support search and secure operations prior to facility operations. 10
7.6 SF6 Inhibit operation of radiation generating devices upon detected high radiation dose rates in an occupied area 10
7.7 SF7 Deter unauthorized entry to exclusion areas 10

7.8 SF8 Provide visual indications of unsecured safe, secure safe, and unsafe radiological enclosure status 11

7.9 SF9 Provide audible warnings of pending unsafe status within a beam enclosure 11

7.10 SF 10 Activate audible and visual alarms when the indicated oxygen level in monitored areas drops below 19.5% by volume. 11

8 General PSS Requirements 11

9 Specific Requirements 13

9.1 Critical Devices 13

9.2 Access Controls 15

9.3 Safety Interlock System (SIS) Requirements 16
9.3.1 SIS Trip Functions: 19

9.4 Software Requirements 20
9.4.1 Application Software 20
9.4.2 Utility Software 21

9.5 Operational Requirements 22
9.5.1 Segmentation 22
9.5.2 Operational Modes 23
9.5.3 Operator Interface 23
9.5.4 Installation and Commissioning 24
9.5.5 Test and Maintenance 25
9.5.6 Modifications 26
9.5.7 Decommissioning 26
9.5.8 Management and Staffing 27

Part One: Generic Requirements

1 Introduction

The Thomas Jefferson National Accelerator Facility (JLab) is a U.S. Department of Energy (DOE) research facility operated by Jefferson Science Associates, LLC. The mission of JLab includes fundamental research in to the understanding of the standard model of physics as well as development of supporting technologies that aid in this mission. Two major accelerator facilities occupy the campus:

- Continuous Electron beam Accelerator Facility (CEBAF)
- Free Electron Laser (FEL)

In addition to the two major facilities, support operations include research and production facilities for electron sources and superconducting radio frequency (SRF) components. Like comparable industrial facilities, JLab operations pose involve hazards that must be mitigated in order to ensure safety of the workforce and general public. The governing document describing the hazards and mitigations is the JLab Final Safety Assessment Document (FSAD). The FSAD describes in general terms methods of hazard controls including administrative and engineered systems.

1.1 Safety Systems

Engineered safety systems are used at Jefferson Lab as one method to reduce risks, presented by the operation of accelerator components, to a level that is acceptable to the U.S. Department of Energy and the Lab management. Personnel Safety Systems (PSS) reduce the risk of personnel exposure to harmful prompt ionizing radiation, non-ionizing radiation, electrocution, and oxygen deficiency.

Safety systems are one of many layers of protection implemented to ensure safety of personnel. Other layers, such as passive shielding, locked doors, signs, sound electrical/mechanical design, operator training, and so on are used in conjunction with safety systems to reduce the risk of injury to personnel from high risk to acceptable or negligible. The FSAD qualifies risk by use of a risk matrix. In the matrix, one axis is “Maximum Consequences” and the perpendicular axis is “Probability of Occurrence.” Intersections of varying levels of consequence and probability are assigned risk code levels. The risk code levels are then determined to be acceptable or unacceptable. Over the life of the facility, risk code 0 and 1 are considered acceptable and risk codes 2, 3, and 4 are considered unacceptable.

At Jefferson Lab this means that processes that are evaluated as risk code 2, 3, or 4 must be mitigated to risk code 0 or 1.[1] The higher the risk code, generally the more safety layers are required for mitigation. The personnel safety systems are one of those layers.

JLab safety systems share the following characteristics:

- They mitigate risks to the general worker within a controlled area.
- They are based on Electrical/Electronic/Programmable Electronic technology.
- They act to sense a dangerous condition.
- They automatically take action to alert personnel to the presence of a hazard, and in most cases act to mitigate the hazard.

The individual safety systems described in subsequent parts of this document give detail requirements for each system and function. Table 1 gives an overview of areas in the JLab complex where SSG designed safety systems are used and the types of hazards present.

Hazard / Area	Prompt Ionizing Radiation	RF non-Ionizing Radiation	Laser Non-ionizing Radiation	Electrocution	Oxygen Deficiency
CEBAF	✓	✓	✓	✓	✓
FEL	✓	✓	✓	✓	✓
Injector Test Cave	✓		✓	✓	
Cryomodule Test Area	✓	✓			✓
Vertical Test Area	✓	✓			

Table 1 JLab Areas Using Personnel Safety Systems

There are other small labs located throughout the JLab complex, such as the ARC and EEL buildings, that incorporate special purpose safety systems. These systems are designed and maintained by the current occupant of the lab and are not within the scope of this document.

2 Scope

This document includes the general requirements for the CEBAF 12GeV upgrade personnel safety systems designed and maintained by the Jefferson Lab Safety Systems Group. The Personnel Safety Systems are designed to prevent harm to personnel in or near an accelerator area. Safety Systems may be designed to mitigate other hazards as required.

In the context of this document, potentially harmful is defined as follows:

- Prompt ionizing radiation dose rate in excess of 5 mrem per hour up to Mrem/hr
- Prompt ionizing radiation dose in excess of 15 rem in any hour
- Prompt radio frequency radiation in excess of the frequency dependent limits given in IEEE STD C95.1 1999

- Laser radiation in excess of the wavelength dependent limits given in ANSI/Z136.1
- Exposed Class II and III electrical hazards of >50 V and > 5mA

Unless otherwise noted in specific requirements a PSS design will not address the following issues:

- Radiation from activated components.
- Electrical shock hazards other than from the operation of the guns and large arc dipole magnets.
- Protection of the general public from radiation doses less than that for trained Jefferson Lab radiation workers. (See Jefferson Lab Radcon Manual.)
- Non-PSS machine hardware from beam related damage.
- Damage to Beam Dumps.
- Contained Beam Loss
- Malicious intent to defeat or circumvent the PSS
- Explosive gas hazards.
- Activation of exhaust fans.
- Exposure to cryogen hazards.

All of these areas are addressed by JLab radiological and EH&S policy and procedures and do not require an active protection system like the Personnel Safety System.

In this document requirements are given in tabular form. Each requirement has a unique identifier.

3 Mission of the PSS

The mission of the Jefferson Lab Personnel Safety Systems is to protect personnel from hazards that arise directly from routine operation of accelerator components. Typically the hazard is generated remotely from the hazardous energy source. Examples are:

- Beam generated by a high voltage electron gun in the injector presents a hazard to other areas
- Magnets, powered by remote box power supplies, presents a hazard to personnel in tunnel
- RF systems, powered by High Power Amplifiers in above ground service buildings, generate radiation hazards in the tunnel

4 Design Basis

The design basis for the personnel safety systems is contained in the references and standards given in the following section.

DB1	PSS designs shall be based on accepted good practices for D.O.E. accelerator facilities and general industry with similar hazards.
DB2	PSS designs shall be subjected to peer review as one method of verifying accepted good practice.

5 References & Standards

This section contains a number of references, regulations, and standards implemented fully or in part at JLab. In the event of a conflict between Industrial and Laboratory standards, the Laboratory standard supersedes the industrial standard.

5.1 ANSI (American National Standards Institute)

- ANSI C95.1 IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz
- ANSI Z136.1 Safe use of Lasers

5.2 IEC (International Electro-technical Commission)

- IEC 61508 Parts 1-3 Functional Safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61511 Part 1 Functional safety – Safety instrumented systems for the process industry sector
- IEC 62061 Safety of machinery - Functional safety - Electrical, electronic and programmable electronic control systems

5.3 U.S. Department of Energy Orders

- DOE Accelerator Safety Order 420.2b
- DOE Accelerator Safety Order 420.2b Guidance

5.4 U.S. Code of Federal Regulations

- 10CFR835 Occupational Radiation Protection
- 10CFR851 Worker Health and Safety Program

5.5 National Council on Radiation Protection (NCRP)

- NCRP Report 88: Radiation Alarms and Access Control Systems
- NCRP Report 144: Radiation Protection for Particle Accelerator Facilities

5.6 International Atomic Energy Agency (IAEA)

- IAEA Report 188: Radiological Safety Aspects for the Operation of Electron Linear Accelerators
- IAEA Report 283: radiological Safety Aspects of the Operation of Proton Accelerators

5.7 National Fire Protection Association (NFPA)

- NFPA 70E Standard for Electrical Safety in the Workplace, 2004 Edition
- NFPA 79 Electrical Standard for Industrial Machinery, 2007 Edition
- NFPA 101 Life Safety Code, 2006 Edition

5.8 International Society for Automation (ISA)

- ANSI/ISA RP92.2 Operation and Maintenance of Oxygen Monitoring Systems

5.9 Jefferson Laboratory requirements, Standards, and Guidelines

- Jefferson Lab EH&S Manual
- Appendix 2410-T2 TJNAF Work Smart Standards Set
- Chapter 3210 Hazard Identification and Characterization
- Chapter 6200 Jefferson Lab's Electrical safety program
- Chapter 6310 Ionizing Radiation Protection
- Appendix 6310-T2 Prompt Radiation Control Policy
- Jefferson Lab Personnel Safety System 12GeV Systems Requirement Document
- Jefferson Lab Quality Assurance Plan

5.10 Jefferson Lab Reports and Notes

- Hall D Beam Containment Proposal
- S01-001 Personnel Safety System Configuration Control Policy
- SSG-UG-01-100 SSG Documentation Numbering Guidelines
- CEBAF PSS Users' Manual
- Safety Systems Documentation Numbering Guidelines
- CEBAF-TN-85-015 Radiation and safety assessment documentation
- CEBAF-TN-86-058 Workshop on radiation safety
- CEBAF-TN-88-073 Proposal for a safety and interlock system for CEBAF
- CEBAF-TN-89-172 Configuration of the switchyard and beamlines for ensuring safety of beams
- CEBAF-TN-89-188 Overview of the accelerator Personnel Safety System
- CEBAF-TN-90-233 Workshop on personnel safety interlocks
- CEBAF-TN-90-228 CEBAF personnel access and safety system – access control system
- CEBAF-TN-90-253 CEBAF Personnel Safety System PLC failure modes and effects analysis
- CEBAF-TN-93-012 Personnel Safety System: Proposal for segmentation of the accelerator tunnel and its interlock systems
- TN-95-028 Description of the CEBAF Personnel Safety System

6 Safety Assessment Document (SAD) Requirements

The JLab Safety Assessment Document gives an overview of the types and magnitude of hazards associated with operation of the CEBAF and FEL accelerators. In addition, safety constraints for facility operations are given as Operation and Safety envelopes. Operations and Safety envelopes for the PSS cover requirements for beam power, radiological exposure, operations staffing, and degraded functionality.

6.1 Operations and Safety Envelope

SAD1	The CEBAF and FEL PSS shall be designed and operated in a manner consistent with the approved Operations and Safety envelopes.
SAD2	Other PSS systems shall be designed and operated to meet the applicable sections of the JLab EH&S manual.

6.2 Certification and Test

SAD3	PSS systems shall be certified and tested at an interval consistent with achieving the required safety integrity level (SIL) or to meet regulatory requirements. In the event of a conflict the more conservative test interval shall be used.

Accelerator	Operations Envelope	Safety Envelope
CEBAF	Twice per calendar year, no less than 4 months and more than 8 months between two certifications.	Once per calendar year
FEL	Twice per calendar year, no less than 4 months and more than 8 months between two certifications.	Once per calendar year
Other Machines	As required to meet safety reliability goals.	Not applicable

Table 2 Certification Interval

6.3 Staffing

SAD4	Personnel performing administrative PSS procedures shall be trained and certified as competent to perform the procedures.
SAD5	Personnel Safety Systems supervising secured PSS areas shall be under the control of trained and certified personnel at all times.

6.4 Fault Tolerance

SAD6	The PSS shall meet or exceed the fail-safe requirements defined for the safety integrity level (SIL) for a designated safety function.
SAD7	Personnel Safety Systems shall be able to carry out the intended safety functions with a full functional failure of one leg of a redundant (1oo2) system.

SAD8	PSS design and implementations shall be robust against common mode failures.
SAD3	Operations shall be suspended in any area where a PSS function or device is suspected of being defective or compromised. Operations shall not recommence until the problem is fixed and recertified or it is determined that the PSS is performing as designed.

7 Safety Functions

Table 4 lists the primary safety functions and associated Safety Integrity Level (SIL) to be achieved by the Personnel Safety Systems in performing a given safety function. Other safety functions may be specified for a specific application. The SIL (Table 3) describes the probability of dangerous failure of the PSS elements that perform the function and is defined in IEC1508.

Safety Integrity Level (SIL)	**Continuous Demand** Probability of dangerous failures, h^{-1}	**Low Demand** Average probability of failure on demand
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$

Table 3

Function ID	Safety Function	Required SIL
SF1	Prevent beam transport from exclusion to occupied areas	3
SF2	Shut off interlocked devices when physical barriers between personnel and hazards are unsecured.	2
SF3	Shut off interlocked devices upon activation of an ESTOP	2
SF4	Shut off interlocked devices in support of administrative access to a secure beam enclosure.	2
SF5	Support search and secure operations prior to facility operations.	2
SF6	Inhibit operation of radiation generating devices when a high radiation dose rate associated with the device is detected in an occupied area	1
SF7	Deter unauthorized entry to exclusion areas	1
SF8	Provide visual indications of unsecured safe, secure safe, and unsafe radiological enclosure status.	1
SF9	Provide audible warnings of pending unsafe status of a beam enclosure	1
SF10	Activate audible and visual alarms when the indicated oxygen level in monitored areas drops below 19.5% by volume.	1

Table 4 Safety Function and SIL Assignments

7.1 SF1 Prevent Beam Transport to Occupied Areas

In multi-segment accelerator facilities such as the CEBAF accelerator, it is possible to operate beam through one segment while an adjacent downstream segment is open for access. Beam transport to the occupied segment must be prevented. Safety layers such as warning devices and locked barriers are ineffective since in this case the beam is coming to the segment, as opposed to personnel attempting entry to a beam operations area.

Critical devices are final elements designed specifically to prevent beam transport to occupied areas. Requirements for critical devices is given in section 10.

SF1.1	The PSS shall prevent beam transport to occupied areas by use of designated critical devices.
SF1.2	For the purposes of verification, SF1 shall be considered a continuous demand safety function.

7.2 SF2 Shut off interlocked devices when physical barriers are unsecured.

JLab Prompt Radiation control policy requires personnel be kept away from prompt ionizing radiation. This is done by operating the PIR source within a secure passive shielding enclosure. Other hazards such as exposed electrical conductors may also exist within a secure enclosure. Barriers in the form of door, gates, movable shielding, ..etc are used to isolate operational hazards from personnel. The PSS must ensure that hazard generating devices are shut off any time personnel can have access to an area.

SF2.1	The PSS shall shut off interlocked devices when physical barriers isolating personnel and hazards are not secure.

7.3 SF3 Shut off interlocked devices upon activation of an ESTOP

A safety system must provide a manual means for emergency shut down. An emergency shut down may be performed by personnel in a secure enclosure or by operators within control facilities.

SF3.1	The PSS design shall include manually activated emergency crash switches (ESTOP) accessible to personnel in controlled areas.
SF3.2	The PSS design shall include manually activated emergency crash switches (ESTOP) in control rooms.
SF3.2	The PSS shall shut off all interlocked devices upon activation of an emergency crash switch (ESTOP)
SF3.3	The PSS shall shut off interlocked devices within 0.5 seconds of activation of an emergency crash switch.
SF3.4	PSS crash switches shall be readily identifiable by personnel with Jlab basic safety training

7.4 SF4 Inhibit operation of interlocked devices in support of secure administrative access.

Large facilities require safe access to a secure area; however the safety layer normally provided by a search and secure operation is no longer in place. In this case an additional interlock function coupled with a closely supervised administrative operation must be provided.

SF4.1	The CEBAF and FEL PSS shall have a secure administrative access mode (e.g. Controlled Access) whereby personnel can gain access to a secure beam enclosure under a closely supervised administrative procedure.
SF4.2	PSS systems other than the CEBAF and FEL are not required to have an administrative access mode.
SF4.2	During a secure access, each person entering the beam enclosure shall carry a token interlocked through the safety system.
SF4.4	The PSS shall inhibit operation of interlocked equipment if any token is in service.

7.5 SF5 Support search and secure operations prior to facility operations.

The transition from an open access to a secure area is a critical administrative procedure before permitting operation of hazardous devices within the area. Search and secure operations (Sweeps) require monitored access and a structured search pattern. Predefined PSS functions assist in the administration of a search and secure operation.

SF5.1	The PSS design shall include search and secure stations that must be armed in a predefined pattern before an area can transition from an occupied to an exclusion area.
SF5.2	The PSS search and secure function shall ensure that an area cannot be switched to an exclusion mode while personnel are within the beam enclosure.

7.6 SF6 Inhibit operation of radiation generating devices upon detected high radiation dose rates in an occupied area

Secure enclosures are used to isolate personnel and operational hazards. However, in the case of prompt ionizing radiation, shielding may not be 100% effective under all circumstances. Radiation monitors are placed in areas most likely to see elevated levels. Interlocks based on measured dose rate are provided to the PSS. In addition to PIR from beam operations, operation of radiation generating devices such as cryomodules may produce elevated levels outside barriers.

SF6.1	The PSS shall shut off interlocked radiation producing devices in any occupied area where radiation monitors detect dose rate in excess of Jlab radiological limits. *Note: this only applies to devices that are capable of contributing to the hazard in the occupied area.*
SF6.2	Radiation monitoring equipment, placement, and trip thresholds shall be under the exclusive control of the Jlab radiological control group (RadCon).

7.7 SF7 Deter unauthorized entry to exclusion areas

In addition to interlocking barriers, it is important to reduce the challenge rate to secure areas. Challenges may come from attempted entry or by natural phenomenon such as wind and thermal cycling. Locked barriers are one safety layer to prevent unauthorized entry.

SF7.1	The PSS shall provide one of the following to prevent unauthorized entry in to an exclusion area: • Automated door locks under the exclusive control of the PSS. • Manually locked doors whose locked/unlocked status is monitored by the PSS. *Note: This safety function is intended to address challenges to the safety system from attempted entry to a secure area. SF2 and SF4 address the interlock function of breech of a secure area.*
SF7.2	The PSS shall activate visual warning devices outside access points to a secure area.

7.8 SF8 Provide visual indications of unsecured safe, secure safe, and unsafe radiological enclosure status

Personnel must be alerted to an unsafe state in order to know to activate an ESTOP.

SF8.1	The PSS shall provide visual indications of the safe/unsafe status of a radiological enclosure.

7.9 SF9 Provide audible warnings of pending unsafe status within a beam enclosure

As an additional safety layer, personnel must be alerted to pending unsafe operations within a secure area. The warning should be sufficient to allow personnel to find and operate ESTOPs and/or to exit the area.

SF9.1	The PSS shall provide an audible warning before changing the status of the beam enclosure from a safe to an unsafe state.

.

7.10 SF 10 Activate audible and visual alarms when the indicated oxygen level in monitored areas drops below 19.5% by volume.

The large inventory of cryogens at Jefferson Lab present significant oxygen deficiency hazards. In addition to highly reliable containment systems, monitoring of affected areas is required. The PSS provides oxygen monitoring and alarm systems. Alarm thresholds are based on OSHA and ACGIH requirements for confined space monitoring.

SF10.1	The PSS shall monitor the oxygen level in areas determined to be potential oxygen deficiency hazard (ODH) areas. *Note: While ODH monitoring systems are a PSS function, they should be separate from safety interlock systems where possible.*
SF10.2	If the detected oxygen level falls below 19.5 % the PSS shall activate audible and visible alarms both within an area and at the entrance to such areas.
SF10.3	The determination for the need for an ODH monitoring system shall be made by the Group Leader for Cryogenic systems or their designee.

8 General PSS Requirements

The following requirements are generic to personnel safety systems used at Jefferson Lab.

GR1	The PSS shall provide access control, interlock, and alarm devices, which when coupled with other safety layers, reduce the risk of a defined accident to risk code 0 or 1.
GR2	Critical devices shall be used to prohibit beam transport from an operational area to an occupied area.
GR3	A PSS access control system (ACS) shall be used to establish and maintain barriers between personnel and operational hazards.
GR4	A PSS Safety Interlock System (SIS) shall be used to mitigate personnel exposure to hazardous energy from devices interlocked through the PSS.
GR5	The determination of the inclusion or exclusion of devices interlocked through the PSS shall be made during the hazard assessment for each facility.
GR6	Primary Safety Systems shall fail to a safe state or condition. *Note: Primary safety systems are those systems that are critical to performing SIL2 and SIL3 safety functions.*
GR7	The fail-safe state for each PSS device and interface shall be defined.
GR8	Unless otherwise justified in writing, the fail-safe state of PSS controls shall be zero volts.
GR9	The status of any hazardous device which is interlocked through the PSS shall be sensed by the PSS.
GR10	If the indicated status of a hazardous device does not agree with the permitted PSS state, the PSS shall default to the fail-safe state.
GR11	PSS systems for a PSS operational segment (areas) shall have control over all devices which could present a hazard to the segment or control over critical devices that protect the segment.
GR12	The PSS shall provide a means for human initiated emergency shutdown of all hazardous equipment that can affect an access control area (e.g. ESTOP).
GR13	The PSS shall be robust against common failure modes including loss of power, short or open circuits, communication errors, and mechanical damage.

GR14	The PSS mean time to repair shall be consistent with the specified safety availability.
GR15	Unless otherwise justified in writing, PSS indoor equipment shall be designed for operation in the following environmental conditions: Ground Benign Ambient Temperature: 0 °C to 120 °C Humidity: 10%-95% non condensing Atmospheric Pressure: 0.8 to 1.2 Bar (81 – 121 kPa)
GR16	Unless otherwise justified in writing, PSS outdoor equipment shall be designed for operation in the following environmental conditions: Outdoor equipment Ambient Temperature: 0 °C to 120 °C Humidity: 10%-95% non condensing Atmospheric Pressure: 0.8 to 1.2 Bar (81 – 121 kPa)

9 Specific Requirements

9.1 Critical Devices

Critical devices are specific accelerator or beamline components that are used to ensure the electron beam is either inhibited or cannot be transported into areas where people are present. A critical device can be an individual component or a collection of components. Examples include power supplies, power switches, beam stoppers, beam current monitors, and electron guns. (ref. Jlab EHS&Q Manual Chapter 6311).

Normally the accelerator is operated such that beam is not transported to a closed beam line. However, it is possible to for an operator steer beam to most closed lines and in other cases failure of a non-PSS component can steer beam in to a closed line.

The critical devices must be able to provide the protection function until the error is detected and corrected. Ultimately the critical device may be destroyed by the beam. In this case the failure mode must ensure that continued beam operations are no longer possible, e.g. loss of vacuum.

CD1	At least three critical devices shall be used to prevent beam transport between exclusion and occupied areas.
CD2	The implementation of critical devices shall use at least two diverse technologies. *Note: for clarification, three devices are required; two of the three must be technologically diverse.*
CD3	One of the two critical device technologies must physically block the beam line, i.e. a 'beam block'.
CD4	Each Critical Device shall be able to perform the intended safety function independent of other critical devices. *Note: Additional devices may be used to prevent catastrophic damage to critical devices, e.g. beam current interlocks.*
CD5	A critical device shall be able to withstand maximum beam power indefinitely OR shall fail in such a way as to prevent any further beam transport. *Note: For example, a magnet string is off, preventing beam transport. Continued beam operations would burn a hole in the beamline, venting the line and preventing any beam transport.*
CD6	Accelerator components such as magnet strings shall be acceptable as one type of critical device if the other conditions of this section are met.
CD7	Each PSS chain shall provide a separate Permit to each critical device. An active Permit is required to transport beam past the critical device, e.g. 'beam allowed.'
CD8	Critical devices shall transition between 'beam allowed' and 'beam not allowed' states within one second of the loss of a PSS permit.
CD9	A PSS Permit to a critical device shall enable remote operation of the device. It is not required that the device automatically move to the 'beam allowed' state.
CD10	Unless otherwise justified in writing, the fail-safe state of critical devices shall be to prevent beam transport.
CD11	Critical devices shall incorporate status feedback elements. The status is sensed by both the upstream (operational) and downstream (protected) PSS systems.
CD12	Critical devices shall be logically controlled by both the upstream (operational) and downstream (protected) PSS segment. Both segments must agree and individually grant a permit for the critical device to transition to the "beam allowed" state.

9.2 Access Controls

An Access Control System shall be used to manage ingress and egress for areas that are alternatively access or exclusion areas. Access control systems shall be designed to provide a warning, prevent access, or initiate mitigating action. Components of an Access Control System may include signs, lights, audible signals, physical barriers, interlocks, run/safe switches, pre-start-up notification procedures, emergency shutdown switches (crash buttons), and administrative operating procedures. (ref EHS&Q Manual Chapter 6311)

Access Control Requirements

AC1	The PSS shall facilitate establishing and maintaining secure access and exclusion areas.
AC2	The PSS shall monitor the status of all doors and movable shielding that allow access to secure areas.
AC3	No access to a radiation enclosure shall be permitted in an “Unsafe” state. If any interlocked door is opened while the PSS is in an “Unsafe” state, the PSS system will drop.
AC4	The PSS shall logically require establishing an exclusion area in the beam enclosure prior to permitting operation of a hazardous device.
AC5	The PSS shall remove permits to hazardous devices upon detection of an unauthorized entry to a secure area.
AC6	The establishment of an exclusion area shall require a visual search and secure (Sweep) of the beam enclosure.
AC7	The search and secure pattern (Sweep) shall follow a designated pattern designed to ensure all beam enclosure areas are observed.
AC8	The PSS shall provide clearly visible status indicators of the “Safe” or “Unsafe” status within the beam enclosure.
AC9	The PSS shall provide an audible warning before transitioning from a “Safe” state to an “Unsafe” state. An administrative announcement over a public address system may substitute for an automated audible warning.
AC10	The PSS shall provide clearly visible status or warning indicators outside of each entrance to the beam enclosure. The status indicators shall be an indication of a potential radiation area.
AC11	The only designated access points to a secure enclosure shall be through dedicated double door access areas. All other doors shall be considered as “emergency exit only.”
AC12	During a sweep or controlled access only one of the two access doors may be in the open position. Both doors open simultaneously shall be considered a breach of the enclosure, resulting in a drop to the safest state.
AC13	Secure access points shall be equipped with PSS door interlocks, interlocked exchange tokens, communication, and remote monitoring equipment.

AC14	PSS visual warnings shall be clearly visible in exclusion areas prior to granting Permits to operate hazardous equipment.
AC15	PSS visual warnings shall be clearly visible outside entrances to exclusion areas when an area is secure.
AC16	PSS audible warnings shall be activated in exclusion areas prior to granting Permits to hazardous equipment. Note: Public Address Announcements are acceptable as audible warnings.
AC17	The PSS shall inhibit transition from the “safe” state to an “unsafe” state if the status of the token is out/unknown.
AC18	The PSS shall impede entry into an exclusion area by use of electrical or mechanical door locks.
AC19	All mechanical locks shall use one unique key under the control of the facility manager.
AC20	All electrical locks shall automatically engage when the PSS is in an “Unsafe” state.
AC21	Unless justified in writing, PSS access controls shall not impede life-safety egress from a beam enclosure.

9.3 Safety Interlock System (SIS) Requirements

A Safety Interlock System (SIS) is used to prevent operation of accelerator equipment when personnel could otherwise be exposed to operational hazards. A SIS shall be used to mitigate any prompt ionizing radiation source capable of generating a high radiation area (> 100 mrem/hr @ 30 cm). Additionally, it shall be used for any prompt ionizing radiation source capable of routinely generating a radiation area (> 5 mrem/hr @ 30 cm) (ref EHS&Q Manual Chapter 6311).

*.

The SIS shall de-energize interlocked equipment if one or more of the following conditions exist:

- Access Control Fault
- Activation of an ESTOP
- Excessive radiation dose rate detected outside the exclusion area
- Status of interlocked equipment is not consistent with the state of the conditions permitted by the SIS.
- SIS element is in an ambiguous or indeterminate state
- SIS logic is in an ambiguous or indeterminate state
- An RF system transmission line is detected as “Open”

The SIS shall be capable of independently sensing hazardous conditions and shutting off hazardous energy sources if such conditions are present, regardless of the status of any other control or sensing function. The SIS shall be designed to adequately mitigate a credible accident or condition.

PSS Safety interlock systems are typically composed of sensors, logic devices, and final control elements. The sensor monitors for a given condition. The logic element combines the information from several sensors and decides if it is acceptable to operate a hazardous energy source. A final element isolates the hazardous energy from personnel.

SIS Requirements

SIS1	Unless justified in writing, the SIS shall be implemented with 2 independent (redundant) chains with 1 out of 2 (1oo2) shutdown capability.
SIS2	The two SIS divisions (chains) shall extend from the sensor to the final device.
SIS3	Each division shall remain independent of the other from the field sensing device up to the final control element.
SIS4	Control and status signals of any equipment not under the direct configuration control of the PSS group shall be electrically isolated from SIS equipment.
SIS5	SIS equipment and wiring shall be located in dedicated PSS racks, conduit, or cable tray.
SIS6	All SIS interlock functions shall be safe against single chain undetected failures.
SIS7	No single chain failure shall result in the ability to energize a hazardous device while personnel may be exposed to a hazard otherwise mitigated by the SIS.
SIS8	The SIS system shall be designed to reduce the risk of hazards resulting from unauthorized access to an enclosure to a risk level 0 – Little to no consequences/Extremely unlikely.
SIS9	The SIS system shall be designed to reduce the risk of exposure to high power microwave radiation to level 0 – Little to no consequences/Extremely unlikely.
SIS10	The SIS shall not be used to provide the normal on/off control of an interlocked device.
SIS11	The PSS shall not automatically reset once a tripped interlock is restored. A manual reset by a qualified operator is required.

[*] JLab EH&S manual chapter 6311 “Prompt Radiation Control Measures”

	ACTION TAKEN					
FAULT	**Drop Beam Permit**	**Drop Sweep**	**Shut off RF Permits**	**Shut off Magnet Permits**	**Remove Critical Device Permits**	**Lock Doors and Gates**
Acess Control Fault	✓	✓	✓	✓	✓	✓
ESTOP Activation	✓	✓	✓	✓	✓	✓
RF Waveguide Interlock	✓		✓			
Status of Interlocked Device inconsistent with PSS State	✓	✓	✓	✓	✓	✓
Radiation Detector Alarm	✓		✓			
Exchange Key Removed- Controlled Access Allowed	✓		✓	✓		
Exchange Key Removed- Other than Controlled Access	✓	✓	✓	✓	✓	✓

Table 5 SIS Actions

9.3.1 SIS Trip Functions:

ID	Description	Action	Time to Reach Safe Condition	Reset Requirement
TF1	Tunnel Access Control Violation	• Shut off all permits • Drop Critical Devices • Drop Sweep	< 1 second	• Error Resolved • Reset Access Controls • Resweep
TF2	ESTOP Activation	• Shut off all permits • Drop Critical Devices • Drop Sweep • Lock doors and gates	< 1 second	• Manual switch reset • Reset Access Controls • Resweep
TF3	RF Waveguide Pressure Interlock	• Shut off beam • Shut off permits to RF only • System	< 1 second	• Error Resolved • Reset permit
TF4	Status of Interlocked Device Inconsistent with the PSS State.	• Shut off beam • Shut off permits to all devices • Drop Sweep • Lock doors and gates	< 3 seconds	• Error Resolved • Reset permit
TF5	Radiation Detector Alarm	• Shut off beam	< 1 second	• Error Resolved • Reset Access State
TF6	Exchange Token Removed (Controlled Access State)	• Shut off beam • Shut off all permits • Drop Critical Devices • Prevent transition to unsafe state	NA	• Replace Key
TF7	Exchange Token Removed (Unsafe State)	• Shut off beam • Shut off all permits • Drop Critical Devices • Drop Sweep • Lock doors and gates	< 1 second	• Error Resolved • Reset Access Controls • Resweep
TF8	Critical Device in incorrect or unknown state	• Shut off beam • Shut off all permits • Drop Critical Devices • Drop Sweep • Lock doors and gates	< 5 seconds	• Error Resolved • Reset Access Controls • Resweep

Table 6 SIS Trip Functions, Timing, and Reset requirements

9.4 Software Requirements

PSS implementations typically use three types of software:

- Application (user) Software
- Utility (Application development) software
- HMI software

Application software is the user program that carries out the desired logic function. The application is developed using utility software that translates the user program in to code to be executed by the target logic controller. The utility program also is used to configure programmable hardware and to map software variables (tags) to physical inputs and outputs.

Errors in software specifications or implementation can lead to systematic failure of the PSS. Human Machine Interface (HMI) software is used to report PSS status to a centralized operator station. Although HMI software is not used for control of safety functions, incorrect software implementation can lead to unnecessary challenges to the safety interlock system.

9.4.1 Application Software

SR-AS1	PSS applications shall be based on a written software requirement specification (SRS) based on IEC61511 chapter 12.
SR-AS2	Unless otherwise approved by the Safety Systems Group Leader, PSS interlock programs shall be written using a limited variability language. *Note: examples of limited variability languages are ladder logic and function block diagrams.*
SR-AS3	Programs for safety certified hardware shall use only certified safety software functions for SIL2 and 3 safety functions.
SR-AS4	Personnel developing PSS software applications shall be formally trained and proficient in the following: • Safety Software programming techniques • The utility software for the target logic device • Software system safety • Hazards and risks of software based systems • The specific safety functions to be implemented in the safety system
SR-AS5	Each division of a redundant PSS system shall be programmed by a separate individual. Each individual shall use the SRS for the performance requirements of the program.
SR-AS6	PSS software shall be fully validated against the SRS before functional tests.

SR-AS7	Software programs shall be validated with all hazardous devices disabled.
SR-AS8	Software testing shall cover all expected inputs and outputs (data boundaries).
SR-AS9	Software testing shall cover anticipated extremes system performance: • Input Timing • Output Timing • Throughput Timing • Communications • Extreme values for analog signals
SR-AS10	Each PSS software programmer shall fully document their PSS programs.
SR-AS11	Software forces shall not be used in a PSS program.

9.4.2 Utility Software

SR-US1	Utility software shall be approved by the hardware manufacturer for use with their system.
SR-US2	Utility software shall, at a minimum, support ladder diagram programming.
SR-US3	Utility software shall include diagnostic and troubleshooting functions.
SR-US4	Utility software shall be capable of on-line and off-line operation.
SR-US5	Utility software shall include utilities for: • Program comparison • Check for forced outputs • Hardware diagnostics • Communication diagnostics • I/O mapping

9.5 Operational Requirements

Operational requirements include activities required to establish and maintain the integrity of a safety system.

9.5.1 Segmentation

OR-S1	In large installations the PSS shall be subdivided in to operational segments.
OR-S2	Each PSS segment shall have sensors, logic elements, and final devices independent from other segments.
OR-S3	Each PSS segment shall have doors, gates, or other barriers such that access to hazards is prevented when the area is in an exclusion mode.
OR-S4	Barriers between PSS segment shall be placed to maximize distance and shielding to hazardous devices within an adjacent segment.
OR-S5	Placement of PSS radiation barriers shall be justified by the JLab radiological control group (RadCon).
OR-S6	Barriers between PSS segments shall be interlocked and locked by the PSS. *Note: this does not apply to fixed barriers like fencing or shield walls with no ready means for access beyond the barrier.*
OR-S7	Fixed PSS segment barriers such as fencing or shield walls shall completely block access beyond the fence or wall. *Note: this means that a fence in the tunnel used as a PSS barrier must extend floor to ceiling and wall to wall. Cut throughs like those for cable trays should not allow a person to crawl through.*
OR-S8	Unless justified in writing by the Jlab EH&S Director, PSS barriers shall not impede life-safety egress from a PSS segment.
OR-S9	The PSS for each operational segment shall provide permits to interlocked equipment which can create a hazard within the segment.
OR-S10	Each PSS segment shall provide permits to critical devices that allow “beam transport” to the area.
OR-S11	Each PSS segment shall NOT affect the operation of the adjacent segment to the greatest extent possible.
OR-S12	Failure of components within one PSS segment shall not affect the ability of an adjacent segment to perform its safety functions.
OR-S13	The segment housing the beam source shall be the “Master” PSS segment.
OR-S14	All other segments shall report “beam allowed” or “beam NOT allowed” status to the Master segment.

OR-S15	The Master PSS segment shall have final control over the Permits to the primary beam sources. *Note: Primary beam sources are equipment whose primary function is to produce beam. Errant beam sources such as "dark current" are considered prompt ionizing radiation from a radiation generating device, e.g. an RF cavity. Dark current is not a primary radiation source.*

9.5.2 Operational Modes

OR-OM1	PSS logic shall be based on operational modes of the PSS segment, area, or device.
OR-OM2	The PSS modes shall be characterized as "access allowed" (access mode) and "access prohibited" (exclusion mode).
OR-OM3	The PSS shall shut off all interlocked devices within a segment if simultaneous access and exclusion modes are detected.
OR-OM4	Where required, the access allowed and access prohibited modes shall be subdivided further to facilitate operational requirements. *Note: examples of additional modes are:* *Restricted Access (access mode)* *Sweep (access mode)* *Controlled Access (access mode)* *Power Permit (exclusion mode)*
OR-OM5	The PSS shall shut off all interlocked devices when in an access mode.
OR-OM6	If the PSS detects interlocked devices are ON/UNSAFE when in an access mode, the PSS shall shut off all interlocked devices.

9.5.3 Operator Interface

OR-OI1	The PSS design shall provide for centralized operator controls.
OR-OI2	PSS controls for any secure PSS segment shall be supervised by a trained and certified operator.
OR-OI3	PSS operators shall be trained and certified for operation of each PSS system.
OR-OI4	PSS operator training shall include the theory of operation, fault recognition, and recognition of unsafe or unusual PSS operations.
OR-OI5	The Safety Systems Group shall provide operator training materials for all installed systems.

OR-OI6	The Safety Systems Group shall administer safety system operator certification exams.
OR-OI7	Any PSS operation that could result in the energizing of radiation generating devices shall be supervised by a trained and certified PSS operator for that area.
OR-OI8	PSS operator interfaces shall give status of: • Operational Modes • Critical Devices • Access Controls • Safety interlock system inputs and permits
OR-OI9	The PSS operator controls shall incorporate the necessary controls to reset faults before restoring operations.

9.5.4 Installation and Commissioning

OR-IC1	All PSS equipment shall be properly installed by personnel approved by the Safety Systems Group Leader.
OR-IC2	All PSS equipment shall be installed according to approved documentation. If errors with the approved documentation are suspected, the installer shall notify the PSS engineer in charge. The PSS engineer in charge shall make the final determination of the correct installation.
OR-IC3	PSS Systems shall be commissioned by the Safety Systems Group and witnessed and accepted by the area owner before hazardous devices are permitted to operate. *Note: PSS systems and functions may be commissioned in stages as long as the requirements of this section are met.*
OR-IC4	The PSS commissioning shall follow a written commissioning plan. The commissioning plan shall be reviewed and approved by personnel responsible for safety within the PSS area.
OR-IC5	Commissioning activities shall include: • Inspection of proper connection of grounding and power • Verification of expected power loading • Inspection for physical damage • Proper calibration of PSS inputs and outputs • Verification of PSS logic solver operation • Verification of software versions used • Verification of PSS inputs and outputs • Verification of interfaces to non-PSS equipment

OR-IC6	PSS validation (certification) procedure shall follow a written validation plan. *Note: The term "validation" is used for the first functional test of the system. This validation test plan may then go on to be used as a" certification" procedure or incorporated in to an overall certification procedure.*
OR-IC7	PSS Systems shall be validated (certified) by a representative of the area owner before hazardous devices are permitted to operate.
OR-IC8	PSS validation (certification) shall include static and functional tests of all PSS inputs, outputs, and operational modes.
OR-IC9	Validation of new PSS Systems or functions shall include the systems' reaction under both normal and abnormal operating conditions.
OR-IC10	Records of system verification and validation shall be maintained by the Safety Systems Group.

9.5.5 Test and Maintenance

OR-TM1	PSS Systems shall undergo periodic certification (proof testing) as required by the system design (e.g. SIL) or regulatory requirements, which ever is shorter.
OR-TM2	Problems found during certification shall be: • Repaired and retested before operations within the area are allowed **OR** • Removed from service until repairs can be performed
OR-TM3	Certification procedures shall include static and functional tests of all PSS inputs, outputs, and operational modes.
OR-TM4	Certifications shall extend from the sensor to the final element.
OR-TM5	Records of completed certifications shall be maintained by the Safety Systems Group.
OR-TM6	Each PSS system shall undergo periodic maintenance required to maintain the designed safety integrity level.
OR-TM7	Only personnel approved by the Safety Systems Group Leader shall be authorized to work on PSS devices or wiring.
OR-TM8	Operations shall be suspended in an area before any work on a PSS device starts.
OR-TM9	Operations are suspended in any area where a PSS device is suspected of being defective. Operations may not resume until the device is repaired and recertified or it is determined by Safety Systems Group personnel that the device is functioning as designed.

OR-TM10	Any PSS device which is electrically disconnected shall be recertified before operations in an area can commence.

9.5.6 Modifications

OR-M1	Modifications to installed PSS systems shall be planned, reviewed, and approved by the area owner before a change is performed.
OR-M2	The following information shall be included in a review of a proposed PSS change or modification: • Description of the change • The rationale for the change (why is it required) • Hazards and safety functions that may be affected • An analysis of the impact the change may have on the existing SILs • The potential for introduction of new hazards • Proposed tests
OR-M3	Changes to PSS interlocks shall require recertification of the interlock and PSS equipment and functions that are associated with the interlock.
OR-M4	Changes to PSS interlock logic (program) shall require a full recertification of the logic program.
OR-M5	Changes to PSS non-interlock logic (program) shall be reviewed by a PSS engineer. The PSS engineer shall determine the extent of testing required. At a minimum all inputs, outputs, and functions associated with the logic affected by the change shall be tested.
OR-M6	Bypassing of safety interlock functions shall only be allowed by the Safety Systems Group Leader if the following conditions are in place: • A PSS jumper request form is submitted and approved by cognizant management • Documented equivalent measures are in place that make the safety system function unnecessary. *Note: For example, an RF waveguide is blanked off, making the PSS safety function (radiation mitigation) unnecessary.*

9.5.7 Decommissioning

OR-D1	PSS Systems may be decommissioned if the system will not be used for an extended period.

OR-D2	The Safety Systems Group Leader shall make the determination if a PSS system will be decommissioned.
OR-D3	Hazardous equipment interfaced to the decommissioned PSS shall be disabled or administratively locked OFF using a lock under the control of the Safety Systems Group.
OR-D4	Recommissioning of a PSS system shall follow the original commissioning test plan as modified to account for changes to the existing system.

9.5.8 Management and Staffing

OR-MS1	Personnel involved in oversight of personnel safety system activities shall have at a minimum: • Management and leadership training appropriate for management of safety systems • Knowledge of the requirements placed on safety system managers and personnel • Knowledge and training on the regulatory and legal requirements for safety system management • Knowledge and training on the requirements of the JLab EHS&Q Manual regarding the management of safety systems • Knowledge of the residual risk associated with operation of safety systems • Knowledge of the requirements for resource allocation required for maintaining safety system personnel qualifications. • Knowledge of the requirements for resource allocation to maintain installed systems.
OR-MS2	Personnel involved in the line management of personnel safety systems shall have at a minimum: • Management and leadership training appropriate for management of safety systems • Knowledge, training, and experience to enable them to assess hazards and risks • Engineering knowledge, training, and experience appropriate for safety system design • Knowledge, training, and experience in managing complex systems • Knowledge of the requirements for resource allocation required for maintaining a given safety system or function • Knowledge of the residual risk associated with operation of safety systems • Knowledge of the requirements for resource allocation required for maintaining safety system personnel qualifications. • Knowledge of the requirements for resource allocation to maintain installed systems.

OR-MS3	Personnel designing personnel safety systems shall have at a minimum: • Engineering knowledge, training, and experience appropriate for safety system design • Engineering knowledge, training, and experience appropriate for application of programmable safety systems • Safety engineering knowledge and experience • Knowledge of legal and regulatory requirements • An understanding of the potential consequences of an unmitigated event • Knowledge of safety instrumented system design and analysis
OR-MS4	Personnel installing and maintaining safety systems shall have at a minimum: • Technical training and experience appropriate for safety systems • Specific training and experience with installed systems • A basic understanding of the theory of operation of the safety systems

[1] JLab EH&S manual chapter 3210