

**System Requirements Specification
for the
Beamline
Personnel Safety System
(PSS)
of the
Advanced Photon Source
at
Argonne National Laboratory
9700 Cass Avenue
Argonne, Illinois 60439**

WBS x.1.4.1.4.1.30.1

Approved By:

John Carwardine, Associate Division Director,
Electrical Systems, ASD

Date

, Group Leader,
SI, ASD

Date

Mohan Ramanathan, Chairman,
Adhoc Gen-3 PSS committee

Date

Jim Lang,
Radiation Safety

Date

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 3/10/2004
	Generation-3 Personnel Safety System	Page 2 of 29		

Prepared By:

Michael Fagan,
SI, ASD

Date

Reviewed By:

Roy Emerson,
SI, ASD

Date

Jon Hawkins,
SI, ASD

Date

Martin Knott,
ESS, ASD

Date

Nick Friedman,
SI, ASD

Date

John Forrestal,
SI, ASD

Date

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Notification Of Specifications Revision	Page <u>3</u> of <u>29</u>		

(INDEX)

INDEX OF PAGE REVISIONS

PAGE NO.	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
REV. NO.	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

PAGE NO.	16	17	18	19	20	21	22	23	24	25	26	27	28	29	
REV. NO.	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

PAGE NO.															
REV. NO.															

PAGE NO.															
REV. NO.															

PAGE NO.															
REV. NO.															

PAGE NO.															
REV. NO.															

REVISION AUTHORIZATION

REVISION NUMBER	00	01	02	03	04	05	06	07	08
DCN NUMBER									
DATE									
APPROVED BY									

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page 4 of 29		

Table of Contents

1. Introduction	5
1.1 System Purpose	5
1.2 System Scope	5
1.3 Definitions, acronyms, and abbreviations	5
1.4 References	6
1.5 System Overview	7
2. General system description	8
2.1 System Content	8
2.1.1 System Interfaces	9
2.1.2 User Interfaces	10
2.1.3 Hardware Interfaces	11
2.1.4 Software Interfaces	12
2.1.5 Communication Interfaces	12
2.2 System modes and states	12
2.2.1 Experimental Station Functional Modes	12
2.3 Major system capabilities	13
2.3.1 Government mandated ESD capabilities	13
2.3.2 Laboratory mandated ESD capabilities	14
2.3.3 Outside sourced ESD capabilities	14
2.3.4 Implied ESD capabilities	14
2.3.5 Internally generated ESD capabilities	14
2.3.6 Laboratory mandated C&C capabilities	15
2.3.7 Outside sourced C&C capabilities	15
2.3.8 Implied C&C capabilities	15
2.3.9 Internally generated C&C capabilities	16
2.4 Major system conditions	16
2.5 Major system constraints	17
2.5.1 Government mandated ESD constraints	17
2.5.2 Government recommended ESD constraints	17
2.5.3 Laboratory mandated ESD constraints	17
2.5.4 Government mandated constraint on the C&C	17
2.5.5 Outside sourced C&C constraints	17
2.5.6 Government mandated constraint on the physical implementation of the system	18
2.5.7 Laboratory mandated constraints on the physical implementation of the system	18
2.6 User characteristics	18
2.7 Assumptions and dependencies	19
Appendix A Requirements Origin, additions, modifications, and justifications	20
Appendix B	25
Appendix C Constraints Origin, additions, modifications, and justifications	26

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page 5 of 29		

1. Introduction

1.1 System Purpose

This System Requirements Specification (SyRS) contains the requirements for the design, development, manufacturing, and verification of the Personnel Safety System (PSS).

1.2 System Scope

This SyRS is limited in scope to the system requirements of the PSS for all beamlines. For requirements specific to an individual beamline, refer to the User Software Requirements Specification.

The PSS is the name of an independent system whose function is to prevent personnel injury from prompt radiation hazards from experimental beamlines at the Advanced Photon Source (APS). This is accomplished by monitoring and controlling personnel access points into hazardous beamline enclosures and beamline critical devices that prevent prompt radiation from unsecured enclosures. The Systems Interlock Group (SI) of the Accelerator System Division (ASD) is responsible for the development and maintenance of the Personnel Safety System at the APS.

1.3 Definitions, acronyms, and abbreviations

The following are some of the frequently appearing or unique words or phrases used in this document. These definitions are provided as a quick reference for the reader's convenience.

Critical Devices: Specific accelerator or beamline components that are used to ensure that the accelerator beam is either inhibited or cannot be steered into areas where people are present.

Door Open: A door where the closed limit switch is not indicating a fully closed position.

Downstream: The direction defined by the path from the Storage Ring to the end of the last Station of a beamline. The beam flow is from the Storage Ring through the Front End Shutters into and through Station A and then to Station B and so on until the beam encounters either a closed Shutter or a beam stop at the end of the last Station.

Upstream: The direction defined by the path from the end of the last Station of a beamline to the Storage Ring. The direction opposite the flow of the beam.

Shutter Open: A shutter where the closed limit switch is not indicating a fully closed position.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page 6 of 29		

The following are some of the frequently appearing or unique acronyms used in this document. This list is provided as a quick reference for the reader's convenience.

ACIS	Access Control and Interlock System
APS	Advanced Photon Source
ASD	Accelerator Systems Division
BLEPS	BeamLine Equipment Protection System
CPU	Central Processing Unit
C&C	Command and Control
DIW	DeIonized Water
DOE	Department Of Energy
EPICS	Experimental Physics and Industrial Control System
EPS	Equipment Protection System
ES&H	Environment, Safety & Health Manual
ESD	Emergency Shut Down
FEEPS	Front End Equipment Protection System
FOE	First Optics Enclosure
I/O	Input Output
IOC	Input Output Controller (data collection for EPICS)
LAN	Local Area Network
OI	Operator Interface
PS1	Photon Shutter 1
PS2	Photon Shutter 2
PSS	Personnel Safety System
PLC(s)	Programmable Logic Controller(es)
PMD	Programmable Message Display
SAD	Safety Assessment Document
SDD	Software Design Document
SS1	Safety Shutter 1
SS2	Safety Shutter 2
SyRS	System Requirements Specification
VME	Versa Module Eurocard
XFD	Experimental Facilities Division

1.4 References

Government Documents

The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement.

Department of Energy (DOE) ORDER 420.2A, 01-08-01

Accelerator Safety Implementation Guide for DOE O 420.2A, Draft, August 2001

DOE ORDER 5480.25, 11-3-92

DOE GUIDANCE 5480.25, September 1, 1993

DOE ORDER and GUIDANCE 5480.25 are included because they were in effect and referenced when the Safety Assessment Document (SAD) was originally written; it has been superseded by DOE ORDER 420.2, which has been superseded by DOE ORDER 420.2A. DOE ORDER 420.2(A) essentially made the approved SAD the effective regulatory document.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page 7 of 29		

Copies of specifications, standards, drawings and publications required by suppliers in connection with specified procurement functions should be obtained from the contracting agency or as directed by the contracting office.

Non-Government Documents

The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirement.

Environment Safety & Health Manual, Section 5.16 (ES&H 5.16) April 25, 2003, Argonne National Laboratory.

APS Safety Assessment Document (SAD), Rev 1, May 1999, Argonne National Laboratory, Argonne, IL.

Compliance with the following required by SAD:

Stanford Linear Accelerator Center Report 327 (SLAC 327), April 1988, Stanford Linear Accelerator Center, Menlo Park, CA.

National Council on Radiation Protection Report No. 88 (NCRP 88), Issued 30 December 1986, National Council on Radiation Protection.

Technical society and technical association specifications and standards are generally available for reference from libraries. They are also distributed among technical groups and using Federal Agencies.

1.5 System Overview

The Personnel Safety System (PSS) is the access control and safety interlock system for the enclosures (stations) of the prompt radiation (X-ray) beamlines, of the Advanced Photon Source, at Argonne National Laboratory. Its function is to prevent personnel injury from prompt radiation hazards associated with the operation of a beamline. It also incorporates control functions for operation of the beamline.

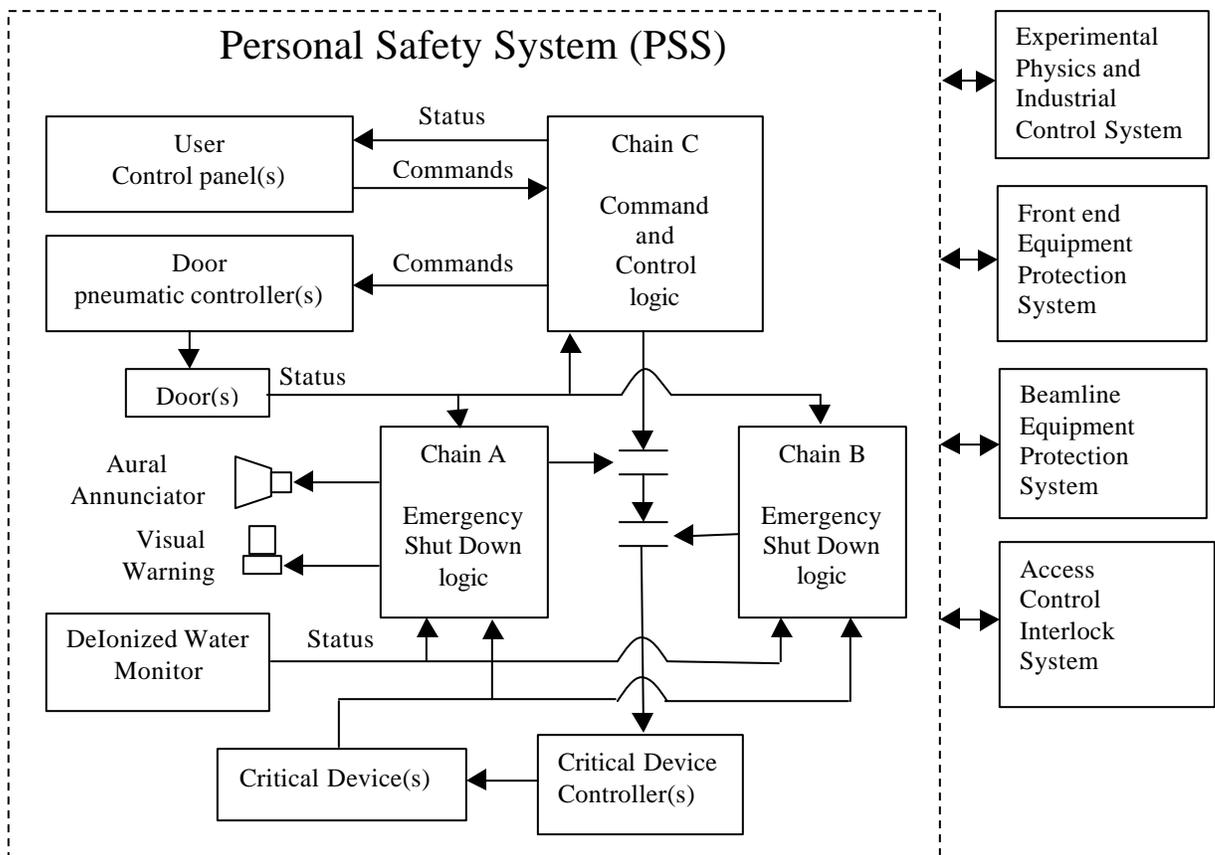
A hazard exists if prompt radiation is allowed into the enclosure without all required shielding in place or while personnel are present within the enclosure. A hazard is also created if, while the prompt radiation is present in the enclosure, access is gained or movable shielding is displaced. To this end the system monitors movable shielding (i.e. doors and interlocked labyrinths), personnel detection (emergency stops, also referred to as crash buttons), and radiation entry (shutter position) of each enclosure of a beamline. The safety interlock portion of the system issues/removes permits to the shutters and storage-ring according to status of the enclosures.

Access control functions are locking/unlocking of doors, opening/closing of powered doors, and guidance/verification of enclosure search. Administrative control functions enforced by the system are control room permit (ACIS FE Shutter permit), floor coordinator key switch (APS Enable) and user key switch (User Enable). Equipment protection is treated the same as administrative control permits (FEEPS FE Shutter Permit and BLEPS Shutter permits). Beamline radiation entry control functions are opening/closing of the shutters.

2. General system description

2.1 System Content

The PSS shall consist of two redundant Emergency Shut Down (ESD) subsystems and a separate command and Control (C&C) subsystem (see system constraints 2.5.1.2 & 2.5.1.3), which in turn interface with systems that control other aspects of the facility. The following block diagram shows the relationships between the major subsystems within PSS and its relationship to the other systems.



	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page 9 of 29		

2.1.1 System Interfaces

These are the existing systems that the PSS interfaces with. There is a brief description of what the system does in relation to PSS and a description of the signals to and from that system.

2.1.1.1 ACIS

The accelerator systems Access Control and Interlock System (ACIS) provide a way for PSS to influence the operation of the next upstream device beyond its direct control, the storage ring
To ACIS

Storage Ring Permit: These are a pair of redundant signals which supply each ESD subsystem a independent mechanism to dump the storage ring in the event the front end shutter in unable to function as a beam stop, or if the beam needs to be removed from an enclosure faster that a shutter can close.

From ACIS

Global Online: This pair of redundant signals indicates a life safety issue, therefore shall go to the EDS subsystems. The beam line is kept "off line" while it is tested and commissioned, or taken "off line" any time it is determined to be unsafe for operation. When operated "off line" all PSS functions will operate normally with the exception of enabling the front-end shutters. When "off line" the ACIS will ignore the loss of the storage ring permit, but will dump the storage ring if it sees any front end shutter open. When "on line" the ACIS ignores the status of the front-end shutters but will dump the storage ring on loss of the storage ring permit.

Front End shutter closed status: The ACIS monitors the closed position limit switches of Photon Shutter 1 (PS1), Photon Shutter 2 (PS2), Safety Shutter 1 (SS1) and Safety Shutter 2 (SS2) and sends redundant status signals that are asserted when the shutters are closed to the EDS subsystems.

Front End Shutter Permit: The ACIS provides an administratively controlled Shutter Permit for the front-end shutters. The C&C shall only open the front-end shutters while this signal is true and will close the shutters if this signal is false.

2.1.1.2 FEEPS

The Front End Equipment Protection System (FEEPS) needs to influence the operation of devices under the direct control of PSS, namely the front end shutters.

To FEEPS

Front End shutter closed status: These multiple signals indicate the safe (beam blocking) position of the front end shutters and lets FEEPS know when a shutter is detected in its fully closed position.

Front End shutter open status: These multiple signals indicate the safe (beam blocking) position of the front end shutters and lets FEEPS know when a shutter is detected in its fully opened position.

From FEEPS

FEEPS Shutter Permit: The front end shutter permit is a permissive and indicates to PSS that it may open the front end shutters, loss of this signal indicates that the PSS should immediately sequence close the front end shutters.

PS1 Open: The backup photon shutter is normally left open, but may be operated by FEEPS through use of the PS1 Open/Close signal. If PSS closes the backup photon stop as result of a fault, it should ignore a request to open it from FEEPS.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>10</u> of <u>29</u>		

2.1.1.3 BLEPS

The BeamLine Equipment Protection System (BLEPS) is similar to the FEEPS, it needs to influence the operation of devices under the direct control of PSS, namely the shutters downstream of the front end shutters.

To BLEPS

BLEPS Shutter Status: These multiple signals indicate the safe (beam blocking) position of the downstream shutters and lets BLEPS know when a shutter is detected in its fully closed position.

BLEPS Shutter Mode: In the case of a mode shutter this signal indicates its currently selected mode.

From BLEPS

BLEPS Shutter Permits: These permits indicate a given shutter may be opened and loss of a permit indicates the need to immediately close that shutter. The PSS will also send signals to the BLEPS to indicate the closed status of any shutter it provides signals for and to indicate the current beam mode.

2.1.1.4 EPICS

The control section of the PSS will provide an interface to the Experimental Physics and Industrial Control System (EPICS). This interface will provide complete PSS status information to EPICS. The C&C control section should accept shutter open/close request, similar to the remote shutter interface, from EPICS.

2.1.2 User Interfaces

2.1.2.1. User Control Panels

The PSS operation will be controlled by user interaction with user control panels. The user panel may contain controls for one or more stations. The user will always be able to close the shutter(s) from any panel.

The panel will also provide the user with an indication of the status of the Global On-Line permit, ACIS FE shutter permit and FEEPS permit enabled signals.

Additionally, the panel will provide the user with indication of the status of the following PSS/Experimental station conditions:

- APS key enabled.
- Station Beam Ready.
- Station Searched.
- The stations shutter/critical device status.

More than one station/shutter status may be indicated to the user on a single panel.

Door Control Panel is incorporated into the touch screen.

The door control panel will provide a positive indication to the user of the following four conditions for each station door:

- The door is open.
- The door is closed.
- The door is locked.
- The door is unlocked.

Additionally, the panel will provide a means to lock and separately unlock each manually operated door.

2.1.2.2 System Control Panel

The system control panel will provide the user with an indication of the system fault status. There are to be two indicators of the fault status which will display three degrees of severity.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>11</u> of <u>29</u>		

The Minor fault status will be indicated by a separate indicator. A positive minor fault indication will be identified by blinking the minor fault indicator at a 1 hertz rate. An absence of a minor fault will be indicated by the same indicator being on but not blinking.

The Serious and Major fault indicator will be the second indicator. A positive fault indication will again be shown by the blinking of the indicator. The PSS system will differentiate between a Serious fault and a Major fault by blinking the indicator at different rates. A Serious fault will be shown by blinking at a slow rate of 1 hertz. A Major fault will be shown by blinking at a faster rate of 2 hertz. The absence of a Serious or Major fault will be shown by the indicator being on but not blinking.

2.1.2.2 Mode Control Panel - Optional

The mode control panel, when present, will enable the user the control of the positioning of a mode shutter. Mode shutters have two operating positions. The Mode shutter may be put into a Mono mode or into a Non-Mono mode. The Non-Mono mode may also be identified as white or pink mode.

The Non-Mono mode is used to lock the shutter open to pass to the down stream stations a high intensity beam. This mode effectively creates a much larger experimental area for high intensity beam. This area extends down stream until a high intensity beam stop is encountered by the beam. This type of beam stop is normally referred to as a white beam stop. Notice, that when in this mode, the area that must be protected by the PSS using the Front End Shutters as the critical device is increased.

The Mono mode is used when the user desires to contain the high intensity beam in the First Optical Enclosure (FOE). When in the Mono mode the mode shutter may be opened and closed by use of the shutter controls on the User Control Panel to control the passage of low intensity monochromatic beam to down stream stations.

2.1.2.3 Automatic Door Controls

For each automatic door on a station there will be an automatic door control unit located conveniently for the user near the door. This control will provide a means to open and close the door using the PSS as the mechanism to operate the door. To close the automatic door a user must provide a continuous indication to the PSS until the door is fully closed. If the user removes the close signal prior to the door fully closing, the PSS will return the door to its full open position.

The automatic door control will provide a positive indication to the user of the following four conditions:

- The door is open.
- The door is closed.
- The door is locked.
- The door is unlocked.

Automatic doors will not respond to a user request to open if there is an upstream shutter open (stations critical device) or if the PSS system has a Serious or a Major fault condition present.

One second after the door has closed the PSS will lock the door.

User Enable Key (many users have asked that this key also lock out door control, could also lockout resetting faults a warnings)

APS Enable Key

Shutter Mode Keys

2.1.3 Hardware Interfaces

There is an understood system hierarchy among the interconnected systems at APS. It is as follow: ACIS, PSS, FEEPS, BLEPS. A higher system should never expose its voltage source to a lower system. This means that the required isolation should be located on the side of the higher system. I.E. If PSS sends a signal to ACIS, it sends a voltage to ACIS to drive the isolation device. And

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>12</u> of <u>29</u>		

when ACIS send a signal to PSS, PSS sends a source voltage to ACIS, which is switch back by the isolation device.

2.1.4 Software Interfaces

None

2.1.5 Communication Interfaces

do we need a description of the EPICS communication interface here?

2.2 System modes and states

2.2.1 Experimental Station Functional Modes.

The functional modes that will be supported by the software contain the basic requirements of the PSS system. Not all mode functions are present in both Chain A and Chain B. However, both software Chains will share the concept of all modes.

Possible add a state diagram.

2.2.1.1. Open Access.

While in an open access mode both Chains software will remove their shutter permits. It will not be possible to open any shutters for any stations.

2.2.1.2. Search and Secure.

The search and secure functions will be performed by Chain A and the search and secure status will be provided to Chain B. **The search and secure process is defined previously in this document.**(needs to include that all doors are closed and end) Chain A and Chain B therefore have information as to this status. Search and secure is a prerequisite to the Beam Ready mode.

2.2.1.3. Restricted Access.

After completing a successful search and secure procedure the station that was searched has a restricted access classification. While a station is in the restricted access mode, the station is ready to receive beam. The restricted access mode will be terminated if any station door is opened or any station emergency stop is pushed in.

2.2.1.4. Beam Ready.

Beam Ready is a significant mode of the PSS. The Beam Ready mode identifies all of the conditions required for a station to receive beam are currently meet. The station will be identified as beam active as soon as the shutters are opened. For the PSS to be Beam Ready for a station the following conditions must be continuously meet:

- The PSS must have the ACIS Global On-Line permit.
- The PSS must have the ACIS FE Shutter permit.
- The shutter manifold pressure must be > 60 P.S.I..
- The PSS must have the shutter permit for the shutter to be opened. The FEEPS permit must be present for the Front End Shutters.

The BLEPS permit must be present for down stream shutters.

- There must not be a Minor fault.
- There must not be a Serious fault.
- There must not be a Major fault.
- The APS key must have been enabled by the floor coordinator.
- The station must be in a Restricted Access Mode.
- If the station is protected by a Mode shutter a valid Mode must be selected.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>13</u> of <u>29</u>		

2.2.1.5. Beam Active.

A station will be identified as Beam Active when it was previously in the Beam Ready Mode and the user has caused the stations shutter (Critical Device) to open and there is beam available at the stations shutter. For example; Station B may be Beam Ready, its shutter may be open, but not be Beam Active until the Front End Shutters are opened. This example requires a shutter for Station B between Station A and Station B.

2.2.2 shutter sequencing

2.3 Major system capabilities

These are the functions the system must perform to be acceptable. For purposes of traceability they have been grouped based on where the requirement originated from. The origins, additions, modifications, and justification for each requirement are contained in Appendix A. Also for easy of design they have also been separated by which subsystem the function should be implemented in. The criteria for determining which functions should be place in which subsystem, along with associated tables, are contained in Appendix B. It should be noted that all requirements applied to the ESD subsystems must be validated annually. All requirements applied to the C&C subsystem shall be verified before the system is commissioned

2.3.1 Government mandated ESD capabilities

The following are requirements placed on the system by government regulations. For the original system, the specific regulations where DOE ORDER 5480.25 and its associated DOE GUIDENCE 5480.25. These are still referenced in the current SAD. They have been superseded by DOE ORDER 420.2 and then by DOE ORDER 420.2A. The guidance for these orders is still in draft form.

2.3.1.1 The ESD subsystems shall signal to ASIC the need to disable the storage-ring operation, on the same PLC scan that detects the fault condition (typically 150 msecs), when the front end shutter position switches indicate any condition other than closed to an unsecured beamline enclosure.

2.3.1.2 The ESD subsystems shall remove permits to shutters while doors are open.

2.3.1.3 An ESD subsystem shall require that search buttons are operated in the correct sequence before beam is allowed in an enclosure.

2.3.1.4 An ESD subsystem shall provide a visual guide to the proper activation sequence of the search buttons

2.3.1.5 An ESD subsystem shall provide both visual and audible indicators of a search in process.

2.3.1.6 The Visual and Audible indicators shall continue for a minimum of 20 seconds after the final door is closed after a search and beam will not be permitted during this time

2.3.1.7 The search sequence shall be required to recur at any loss of door closed status.

2.3.1.8 An ESD subsystem shall provide enclosure status at each entrance to the enclosures. Minimally Open, Beam Ready, Beam Active.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>14</u> of <u>29</u>		

2.3.1.9 The ESD subsystems shall continuously monitor emergency shutdown switches ("crash buttons") that inhibit storage-ring operation when depressed while the associated enclosure is BEAM ACTIVE.

2.3.2 Laboratory mandated ESD capabilities

The following are requirements placed on the system by policies of Argonne National Labs, specifically the ES&H 5.16.

2.3.2.1 The PSS shall send critical status to EPICS for logging.

2.3.2.2 The ESD subsystems shall monitor critical devices for proper operation, and upon detection of improper operation, the beam should be inhibited by operation of other critical devices upstream.

2.3.2.3 Interlock trips shall be reset locally

2.3.3 Outside sourced ESD capabilities

The following are requirements placed on the system by the choice to comply with the following in the SAD; the Stanford Linear Accelerator Center Report 327, and the National Council on Radiation Protection Report No. 88.

2.3.3.1 The ESD subsystems shall signal to ASIC the need to disable storage-ring operation, on the same PLC scan that detects the fault condition (typically 150 msecs), when improper access is gained to a hazardous beamline enclosure.

2.3.3.2 The ESD shall enforce a programmable time limit on the search procedure and securing of the station (closing of the final door).

2.3.4 Implied ESD capabilities

The following are believed to be implied in the previously stated requirements and are simply listed here for completeness.

2.3.4.1 The ESD subsystem shall inhibit the entry of beam into any unsecured beamline enclosure

2.3.4.2 The ESD subsystem shall inhibit the search sequence if any associated emergency shutdown switches ("crash buttons") is depressed.

2.3.4.3 The ESD subsystems will require the search sequence to recur any associated emergency shutdown switches ("crash buttons") is operated.

2.3.4.4 The ESD subsystems shall only permit operation of Photon Stop 2 (PS2) Safety Shutters 1 and 2(SS1 & SS2) while the ACIS Global On-line signal is true.

2.3.5 Internally generated ESD capabilities

The following are additional requirements the group agreed on, that are beyond the mandated functions. These requirements may be modified or removed based on agreement of the design committee.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>15</u> of <u>29</u>		

2.3.5.1 Each ESD subsystems shall output an external watchdog pulse to allow for verification that the subsystem's program is running.

2.3.5.2 Each ESD system shall monitor the external watchdog pulses of the other ESD system, and shall remove permits to shutters when loss of pulse train is detected.

2.3.5.3 The ESD subsystems shall have a hardwired hardware location and software version that the software will validate before the beamline is allowed to operate

2.3.5.4 The ESD subsystem shall only permit shutter operation when there is sufficient air pressure for proper operation (>60psi).

2.3.6 Laboratory mandated C&C capabilities

The following are requirements placed on the system by policies of Argonne National Labs, specifically the ES&H 5.16.

2.3.6.1 The C&C subsystem shall automatically lock all doors to a station at the completion of search and secure.

2.3.7 Outside sourced C&C capabilities

The following are requirements placed on the system by the choice to comply with the following in the SAD; the Stanford Linear Accelerator Center Report 327, and the National Council on Radiation Protection Report No. 88.

2.3.7.1 The C&C shall not command the unlocking or opening of doors while there is beam is present in the enclosure.

2.3.8 Implied C&C capabilities

The following are believed to be implied in the previously stated requirements and serve to keep the C&C in sync with the ESD subsystems.

2.3.8.1 The C&C shall not command the opening of a shutter unless the downstream area has been searched and all associated doors are closed.

2.3.8.2 The C&C shall not command the opening of a shutter till after visual and audible indicators have stopped

2.3.8.3 The C&C shall not command the opening of a shutter if any downstream crash buttons are activated.

2.3.8.4 The C&C shall sequence the shutter closed if downstream crash buttons are depressed while the associated enclosure is BEAM ACTIVE.

2.3.8.5 The C&C shall sequence the shutter closed on loss of associated door closed status.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>16</u> of <u>29</u>		

2.3.8.6 The C&C shall not command the opening of a shutter unless the ACIS Global On-line signal is true.

2.3.8.7 The C&C shall sequence the shutter closed on loss watchdog pulse train.

2.3.8.6 The C&C shall not command the opening of a shutter unless there is sufficient air pressure for proper operation (>60psi).

2.3.9 Internally generated C&C capabilities

The following are additional requirements the group agreed on, that are beyond the mandated functions. These requirements may be modified or removed based on agreement of the design committee.

2.3.9.1 The C&C shall not command the opening of the front end shutters (PS2, SS1, & SS2) unless the ACIS Front End Shutter Permit is true.

2.3.9.2 The C&C shall not command the opening of the Front End Shutter unless the FEEPS permit is true.

2.3.9.3 The C&C shall sequence the Front End Shutter closed on loss of the FEEPS permit.

2.3.9.4 The C&C shall not command the opening of a shutter unless the associated user key is captured.

2.3.9.5 The C&C shall sequence the shutter closed on loss of associated the user key.

2.3.9.6. The C&C shall not command the opening of the front end shutters unless associated enclosure is APS enabled.

2.3.9.7 The C&C shall sequence the shutter closed on loss of the associated APS enable.

2.3.9.8 The C&C subsystem shall provide a logical visual indication of the beamline status on the station control panel

2.3.9.9 The C&C subsystem shall provide beamline shutter controls on the station control panel

2.3.9.10 The C&C shall not command the opening of an integral shutter unless the associated BLEPS permit is true.

2.3.9.11 The C&C shall close an integral shutter on loss of the associated BLEPS permit.

2.4 Major system conditions

These are the capacities the system must be able to handle to be acceptable. The systems I/O, memory, and processing capacities must be able to handle the maximum case design.

See "Standard Beamline Configuration for the Generation 3 Personnel Safety System".

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>17</u> of <u>29</u>		

2.5 Major system constraints

These are constraints placed on the system. They must be followed for the system to be acceptable. For purposes of traceability they have been grouped based on where the requirement originated from. The origins, additions, modifications, and justification for each requirement are contained in Appendix C. Also for easy of design they have also been separated by which subsystem the constraint applies to.

2.5.1 Government mandated ESD constraints

The following are constraints placed on the system by government regulations. (See 2.3.1 for details)

- 2.5.1.1 All signals to controlled devices shall supply power to the device so that common failures (e.g., shorts to ground, open wires, or loss of power) leave the system in a safe, beam-off state.
- 2.5.1.2 The PSS shall have two independent ESD subsystems with separate sensors on all monitored devices, that can cause loss of protection.
- 2.5.1.3 The PSS shall have a separate control subsystem for routine operation of beamlines.

2.5.2 Government recommended ESD constraints

The following are constraints recommended by government regulations. (See 2.3.1 for details) The decision has been made to follow these recommendations. These constraints may be removed if the design committee believes they put undue restrictions on the system.

- 2.5.2.1 Each PSS shall be stand-alone and operate on exactly one beamline
- 2.5.2.2 Where practical, each ESD subsystem shall be programmed by different programmers working independently.

2.5.3 Laboratory mandated ESD constraints

The following are constraints placed on the system by policies of Argonne National Labs, specifically the ES&H 5.16.

- 2.5.3.1 As is reasonable practical, the ESD subsystems shall not perform equipment protection functions.

2.5.4 Government mandated constraint on the C&C

The following are constraints placed on the system by government regulations. (See 2.3.1 for details).

- 2.5.4.1 Mechanisms shall be provided to allow emergency access and egress.

2.5.5 Outside sourced C&C constraints

The following are constraints placed on the system by the choice to comply with the following in the SAD; the Stanford Linear Accelerator Center Report 327, and the National Council on Radiation Protection Report No. 88.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>18</u> of <u>29</u>		

2.5.5.1 The safety interlock systems shall not allow program modification while in operation; they must be put in a programming mode via a key.

2.5.6 Government mandated constraint on the physical implementation of the system

The following are constraints placed on the system by government regulations. (See 2.3.1 for details).

2.5.6.1 The system should be designed such that the ESD portion can be tested independently of the Control subsystem in a non-invasive manner (no signal paths shall be broken).

2.5.6.2 All PSS systems, wiring, and devices shall be clearly labeled to note that tampering is strictly forbidden

2.5.6.3 All PSS circuitry and wiring shall be in secured cabinet, raceways, conduit, or in armored cable not shared with any non-related system.

2.5.6.4 Crash Buttons shall be clearly visible and unambiguously labeled

2.5.7 Laboratory mandated constraints on the physical implementation of the system

The following are constraints placed on the system by policies of Argonne National Labs, specifically the ES&H 5.16.

2.5.7.1 Crash buttons shall require manual resetting.

2.5.7.2 Door closed sensor shall be inaccessible for the outside of the enclosure.

2.6 User characteristics

This section contains assumptions, requirements and constraints involving beamline users behavior.

2.6.1 The user is expected to understand the need for the PSS and not attempt to defeat it.

2.6.2 The PSS must not be used as a substitute for normal beamline safety precautions.

2.6.3 Users must learn to use the system the way the designers and its logic intend it to be used, although they must remember to use their training and experience to evaluate situations and take appropriate action to ensure safety.

2.6.4 Users will make a conscious effort to verify no personnel remains in the enclosure during the search and secure procedure.

2.6.5 Any personnel that may be in an enclosure will understand warning messages and will respond to such warnings appropriately. i.e. press crash button to prevent entry of prompt radiation into the enclosure.

2.6.6 Any personnel that may be in an enclosure will be physically able to respond to warning messages appropriately. i.e. conscious and not immobilized

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>19</u> of <u>29</u>		

2.7 Assumptions and dependencies

The correct operation of the PSS is based on some assumptions about the environment in which the PSS operates.

2.7.1 High-integrity communication exists between PSS and ACIS.

2.7.1.1 ACIS will shutdown Storage Ring on loss of permit.

2.7.1.2 ACIS will provide front-end shutter closed status in an accurate and timely manner

2.7.2 High-integrity communication exists between PSS and Equipment Protection Systems.

2.7.3 Critical Device status inputs reflect true position of critical device.

2.7.4 Critical Devices are aligned correctly in beam path and block prompt radiation.

2.7.5 Critical Devices will close when de-energized.

2.7.6 Door position sensing inputs reflect true position of door.

2.7.7 Labyrinth position sensing inputs reflect true position of labyrinth.

2.7.8 Closed doors and labyrinths have been verified to block radiation.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>20</u> of <u>29</u>		

Appendix A Requirements Origin, additions, modifications, and justifications

For each requirement the supporting mandates or recommendations follow. On occasion the requirement has been made more restrictive or additionally constrained due to other requirements or recommendation sources that have been selected to be followed. Rather than repeat the requirement or modify it in a different section. The requirement remains grouped with its original source.

A.2.3.1.1 The ESD subsystems shall disable the storage-ring operation on the same PLC scan that detects the fault condition (typically 150 msecs)., when the front end shutter position switches indicate any condition other than closed to an unsecured beamline enclosure.

DOE 5480.25 Guidance, Part 1.F., section 2. b (4)(b), "The status of each critical device should be monitored to ensure that the devices are in a "safe" condition when personnel access is allow. ... If the "safe" condition is lost, the beam should be inhibited by operation of other critical devices upstream."

DOE 420.2A Guidance, Chapter II, section C. 3. d. (2), "The status of each critical device should be monitored to ensure that the devices are in a "safe" condition when personnel access is permitted. ... If the "safe" condition is lost, the beam should be inhibited by operation of other critical devices upstream."

The requirement was additionally constrained to meet ALARA (As Low As Reasonably Achievable) radiological exposure requirements.

A.2.3.1.2 The ESD subsystems shall remove permits to shutters while doors are open.

DOE 5480.25 Guidance, Part 1.F., section 2.b. (5). "The entry interlocks should not constitute the normally used means of disabling beam. However, interlocked safety devices should be employed to maintain beams disabled."

DOE 420.2A Guidance, Chapter II, section C. 3. e, "The entry interlocks should not constitute the normally used means of disabling beam. However, interlocked safety devices should be employed to maintain beams disabled."

NCRP REPORT No. 88, section 3.1.5, paragraph 1, "Also, interlocks prevent the production of high levels of radiation unless all of the barriers are in place."

A.2.3.1.3 An ESD subsystems shall require that search buttons are operated in the correct sequence before beam is allowed in an enclosure.

DOE 5480.25 Guidance, Part 1.F., section 2.c. (4), Exclusion areas should be searched before the beam is introduced to insure no people remain inside. ... Search confirmation buttons, or check stations should be placed to ensure that the search team can view all parts of the area."

DOE 420.2A Guidance, Chapter II, section C. 4. d., "Exclusion areas should be searched before the beam is introduced to insure no people remain inside. ...(1) Search confirmation buttons, or check stations should be placed to ensure that the search team can view all parts of the area."

ES&H Chap 5-16, section Hardware Req., paragraph, 13, "There shall be hardware to require a full search-and-secure at startup and after each gate trip. If reset stations are installed, they shall be connected in a sequence that ensures a systematic and thorough search.

NCRP REPORT No. 88, section 3.1.7, paragraph 2, "In large or complex facilities, particularly for those with high-to-extreme potential dose category areas, a through search should be made before operations begin."

SLAC 327, section Features of an Interlock System, item 6, ""Search Confirmation" switches, mounted at appropriate locations along the search path, should also be provided."

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>21</u> of <u>29</u>		

Note: Since this is a system enforced Administrative Control Procedure, it only needs to be in one ESD subsystem.

- A.2.3.1.4 An ESD shall provide a visual guide to the proper activation sequence of the search buttons Internally it was agreed that the system shall give visual guidance to the proper sequencing of the search buttons. Since the search enforcement is already in an ESD subsystem, it was decided to keep the visual guidance in the same subsystem.
- A.2.3.1.5 An ESD shall provide both visual and audible indicators of a search in process.
 SLAC 327, section Features of an Interlock System, item 4, "Inside radiation enclosures, clear visual warning should be given that the accelerators is about to come on."
 SLAC 327, section Features of an Interlock System, item 5, "Audible warning should be given inside accelerator enclosures before the accelerator is turned on."
 Since the pre-introduction warnings must be performed in the ESD subsystem (see next), the decision was made to keep all visual and audible indicators with the ESD subsystems.
- A. 2.3.1.6 The Visual and Audible search indicators shall continue for a minimum of 20 seconds after the final door is closed after a search and beam will not be permitted during this time
 DOE 5480.25 Guidance, Part 1.F., section 2.c. (4)(b), "After an exclusion area is secured, an audible and visual warning should be provided before the beam is introduced"
 DOE 420.2A Guidance, Chapter II, section C. 4. d. (2), "After an exclusion area is secured, an audible and visual warning should be provided before the beam is introduced"
 ES&H Chap. 5-16, section Hardware Req. paragraph 14, " An announcement or other audible warning must sound in the enclosures after the completion of the search and secure procedure for at least 20 seconds to allow safe egress or interlock disablement. Voice warnings are encouraged rather than annunciators.
 NCRP REPORT No.88, section 3.1.7, paragraph 3, "After the search sequence has been completed, a notification should be made that radiation-producing operations will begin."
 SLAC 327 Features of an Interlock System item 7," The interlock system should prevent beams from being turned on until after the search has been completed and acknowledged and the audible and visual warning light cycle has ended."
- A.2.3.1.7 The search sequence shall be required to recur at any loss of door closed status.
 DOE 5480.25 Guidance, section Part 1.F. 2.c. (4)(c), "If entry control is compromised, then the search and warning interval should be repeated before introducing the beam"
 DOE 420.2A Guidance, Chapter II, section C. 4. d. (3), "If entry control is compromised, then the search and warning interval should be repeated before introducing the beam"
 ES&H Chap 5-16, section Hardware Req., paragraph, 13, "There shall be hardware to require a full search-and-secure at startup and after each gate trip.
 NCRP REPORT No. 88, section 3.1.5, paragraph 2, item 3, "The opening of an interlock should trigger a requirement to reinitiate the startup procedure, which would involve searching any controlled access area that may have been opened when the interlock was broken."
- A.2.3.1.8 An ESD subsystem shall provide enclosure interlock status at each entrance to the enclosures.
 DOE 5480.25 Guidance, Part 1.F., section 2.c. (3), "Signs or clearly labeled lights reflecting current exclusion area status should be provided at all entry doors."
 DOE 420.2 Guidance, Chapter II, section C. 4. c., "Signs or clearly labeled lights reflecting current exclusion area status should be provided at all entry doors."
 ES&H Chap 5-16 Hardware Req. paragraph. 8, "Enclosure interlock status indicators are required at each entrance."

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>22</u> of <u>29</u>		

SLAC 327, section Features of an Interlock System, item 4, "Warning lights or annunciation signs should be located outside entrances to accelerator enclosures."

A.2.3.1.9 The ESD subsystems shall continuously monitor emergency shutdown switches ("crash buttons") that inhibit storage-ring operation when depressed while the associated enclosure is BEAM ACTIVE.

DOE 5480.25 Guidance, Part 1.F, section. 2.c. (1), "Emergency shut-off devices, which are clearly visible, unambiguously labeled and readily accessible, should be provided in exclusion areas."

DOE 420.2 Guidance, Chapter II, section C. 4. a., "Emergency shut-off devices, which are clearly visible, unambiguously labeled and readily accessible, should be provided in exclusion areas."

ES&H Chap 5-16 Design Req. paragraph 3, "Emergency shut-off devices (scram switches) that are clearly visible, unambiguously labeled, and readily accessible should be provided by the facility manager, even when interlocks are not required." and section Hardware Req., paragraph 10, "A scram switch, pull-chain, or other emergency power cutoff switch shall be clearly visible, unambiguously labeled, and located within easy reach.

NCRP 88 3.1.6 paragraph 3, "Manually operated emergency shutdown switches, which immediately terminate the production of radiation or move radiation to its shielded enclosure, should be placed conspicuously in areas that contain high-to-extreme potential radiation hazards."

A.2.3.2.1 The PSS shall send critical status to EPICS for logging.

ES&H Manual Chapter 5-16 section Software Requirements paragraph 2, "Data logging of the computer interlock and radiation meters should be preformed in such a way as to allow the data to be used for radiation permits or dose reconstruction."

The ESD subsystems will send their critical status to the C&C sub system, which will forward it the EPICS.

A.2.3.2.2 The ESD subsystems shall monitor critical devices for proper operation, and upon detection of improper operation, the beam should be inhibited by operation of other critical devices upstream.

ES&H Manual Chapter 5-16 section Hardware Requirements paragraph 8, "In those areas where a single primary device is used to ensure safety, status monitoring is required to detect a device failure and to activate a failure mode device."

A.2.3.2.3 Interlock trips shall be reset locally

ES&H Chap 5-16, section Hardware Req., paragraph. 9, "When an interlock has been tripped, it must be possible to resume operation of the radiation-producing device only by manually resetting controls at the position where the interlock has been tripped, and lastly at the main control console."

A.2.3.3.1 The ESD subsystems shall disable storage-ring operation, on the same PLC scan that detects the fault condition (typically 150 msec), when improper access is gained to a hazardous beamline enclosure.

NCRP REPORT No. 88, section 4.4, paragraph 2, "Access control devices should be provided that prevent access and initiate automatic shutdown if access is to a hazardous radiation area is attempted."

This is also implied in 2.3.1.2

The requirement was additionally constrained to meet ALARA (As Low As Reasonably Achievable) radiological exposure requirements.

A.2.3.3.2 An ESD subsystem shall enforce a programmable time limit on the search procedure and securing of the station (closing of the final door).

NCRP REPORT No.88, section 3.1.7, paragraph 2, "The search should require that the searcher activate, within a set time period, a run/safe switch at each of several stations in the area to be

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>23</u> of <u>29</u>		

cleared. If the run/safe switches are not activated within the set time interval, then the sequence must be initiated again."

Since only one ESD subsystem enforces the search requirements (see A.2.3.1.3), only it need enforce the time limit.

A.2.3.4.1 The ESD subsystem shall inhibit the entry of beam into any unsecured beamline enclosure
Implied in 2.3.1.1

A.2.3.4.2 The ESD subsystem shall inhibit the search sequence if any associated emergency shutdown switches ("crash buttons") is depressed.
Implied by combination of 2.3.1.7 and 2.3.1.9

A.2.3.4.3 The ESD subsystems will require the search sequence to recur any associated emergency shutdown switches ("crash buttons") is operated.
Implied by combination of 2.3.1.7 and 2.3.1.9

A.2.3.4.4 The ESD subsystems shall only permit operation of Photon Stop 2 (PS2) Safety Shutters 1 and 2(SS1 & SS2) while the ACIS Global On-line signal is true.

Implied by the definition of the Global On-Line/Off-line signal. A beamline that is Off Line is not considered safe to accept beam.

A.2.3.5.1 Each ESD subsystems shall output an external watchdog pulse to allow for verification that the subsystem's program is running.

The assumption is that the PLC must be running the program to create this software timer function,

A.2.3.5.2 Each ESD system shall monitor the external watchdog pulses of the other ESD system, and shall remove permits to shutters when loss of pulse train is detected.

If one of the ESD subsystem is not running its program, redundant protection has been lost.

A.2.3.5.3 The ESD subsystems shall have a hardwired hardware location and software version that the software will validate before the beamline is allowed to operate.

This is to insure that if code from the wrong beamline or the wrong revision of code is loaded, the beamline will not operate.

A.2.3.5.4 The ESD subsystem shall only permit shutter operation when there is sufficient air pressure for proper operation (>60psi).

A.2.3.6.1 The C&C subsystem shall automatically lock all doors to a station at the completion of search and secure.

ES&H Chap 5-16, section Definitions, "search and secure - the act of searching an area/enclosure to ensure that all personnel have left, and then locking and/or interlocking the area/enclosure."

A.2.3.7.1 The C&C shall not command the unlocking or opening of doors while there is beam is present in the enclosure.

SLAC 327, section Features of an Interlock System, paragraph 4, item 1, "The interlock system should permit a key release or a door opening only when an area is safe to enter."

A.2.3.8.1 The C&C shall not command the opening of a shutter unless the downstream area has been searched and all associated doors are closed.

Implied from 2.3.1.2 and 2.3.1.3, insures no challenge to the ESD system.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>24</u> of <u>29</u>		

A.2.3.8.2 The C&C shall not command the opening of a shutter till after visual and audible indicators have stopped

Implied from 2.3.1.6, insures no challenge to the ESD system.

A.2.3.8.3 The C&C shall not command the opening of a shutter if any downstream crash buttons are activated.

Implied from 2.3.1.9, insures no challenge to the ESD system.

A.2.3.8.4 The C&C shall sequence the shutter closed if an emergency shutdown switches ("crash buttons") is depressed while the associated enclosure is BEAM ACTIVE.

Implied from 2.3.1.9, close the shutters in addition to storage ring dump.

A.2.3.8.5 The C&C shall sequence the shutter closed on loss of associated door closed status.

Implied from 2.3.3.1, close the shutters in addition to storage ring dump.

Implied from 2.3.5.4, keep C&C in sync with ESD subsystems.

A.2.3.8.6 The C&C shall not command the opening of a shutter unless the ACIS Global On-line signal is true.

Implied from 2.3.4.4, insures no challenge to the ESD system.

A.2.3.8.7 The C&C shall sequence the shutter closed on loss watchdog pulse train.

Implied from 2.3.5.2, keep C&C in sync with ESD subsystems.

A.2.3.8.6 The C&C shall not command the opening of a shutter unless there is sufficient air pressure for proper operation (>60psi).

Implied from 2.3.5.4, insures no challenge to the ESD system.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>25</u> of <u>29</u>		

Appendix B

When determining which subsystem a function should be implemented in, the following signal criteria were used as a guide. Then based on which signals a given function required, it is to be placed in that subsystem

Criteria for connection to ESD

If the answer is yes for any of the following questions the corresponding signal must be connected to the ESD portion of the PSS

1. Can this signal (assertion, negation, or loss of) indicate a need to immediately shutdown the beam to "prevent exposure of personnel in excess of the most current DOE standards for ionizing and non-ionizing radiation" DOE 5480.25 par. 9.c.(1)
2. Does this signal
 - a. permit the operation of a critical device as defined by DOE G 5480.25 part 1.F. par. 2.b.(4) {420 part II.C.3 par. d} and require implementation by dual chain as set forth in SAD 3.12.1.3.2.6 or disable the storage ring under conditions set forth in SAD 3.12.2.1
 - b. monitor a critical device as required by DOE G 5480.25 part 1.F. par. 2.b.(4)(b) {420 part II.C.3 par. d (2)}
 - c. or indicate that said device is not operating within normal conditions. An example of operation exceeding normal conditions and the need for protection is given in DOE G 5480.25 part 1.D. par. 3.d. (and part 1.D. par. 2.b.(1)) {420 part I.B.2 par.2 a) and part I.B.2 par 7}
3. When prompt radiation is present, will this signal or device detect an attempt to access or presence of personnel in a Radiological Area as defined by DOE 5480.25 par. 6.1.

All other signal will be considered either administrative as described in SAD 3.12.2, control of non-critical devices, or HMI in nature and will reside in a separate system.

By observing which function a signal is associated with, the function was then placed in the appropriate subsystem.

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>26</u> of <u>29</u>		

Appendix C

Constraints Origin, additions, modifications, and justifications

For each constraint the supporting mandates or recommendations follow. On occasion the constraint has been made more restrictive due to other requirements or recommendation sources that have been selected to be followed. Rather than repeat the constraint or modify it in a different section. The constraint remains grouped with its original source.

C.2.5.1.1 All signals to controlled devices shall supply power to the device so that common failures (e.g., shorts to ground, open wires, or loss of power) leave the system in a safe, beam-off state.

DOE 5480.25 Guidance, Part 1.F., section 2. b. (1), "The protective functions of the interlock system should be fail-safe against routine failures, including loss of power or pressure, open circuits, and shorts to ground."

DOE 420.2A Guidance, Chapter II, section C. 3. a, "The protective functions of the interlock system should be fail-safe against routine failures, including loss of power or pressure, open circuits, and shorts to ground."

ES&H Chap 5-16, section Design Req., paragraph. 6, " Fail-safe designs shall be used when possible." and Hardware Req. paragraph 7, "The design of the safety system shall be such that it cannot be compromised by accidental grounding or the introduction of outside electronic signals."

ES&H Chap 5-16, section Hardware Req., paragraph 4, "The design of the safety system must be such that it cannot be comprised by accidental grounding or the introduction of outside electronic signals."

NCRP REPORT No. 88, section 3.1.5, paragraph 2, item 1, " Interlocks should be "fail-safe"; that is, in their most likely failure modes, they will prevent the production of high radiation levels in potentially occupied areas,"

SLAC 327, section Interlock Design, paragraph 2, "Fail-safe circuits and components should be used whenever practicable. ... In each case, the safety interlock system should react to render the area safe in the event that a key safety component fails or the power is lost."

C.2.5.1.2 The PSS shall have two independent ESD subsystems with separate sensors on all monitored devices, which can cause loss of protection.

DOE O 5480.25 Part 1.F section 2. b. (2), "Interlocks should be arranged so that no single failure will cause a loss of protection"

DOE 5480.25 Guidance, Part 1.F., section 2. b (4)(b), "The status of each critical device should be monitored to ensure that the devices are in a "safe" condition when personnel access is allow. If only one device is used, two separate indication systems should be used"

DOE 420.2A Guidance, Chapter II, section C. 3. d. (2). "The status of each critical device should be monitored to ensure that the devices are in a "safe" condition when personnel access is permitted. If only one device is used, two separate indication systems should be provided"

ES&H Chap 5-16, section Hardware Req., paragraph 4, "There must be two redundant methods monitoring each personnel access point that are not subject to a common mode failure (for example, one pulsed optical sensor set, or one mechanical and one magnetic switch, or two independent mechanical switches). The switches or sensors shall be inaccessible from the "safe" side of the access point. Either redundant method shall be able to force the equipment/facility into a safe condition."

NCRP REPORT No.88, section 3.1.5, paragraph 2, item 2, "Each access control barrier to radiation areas that are classified in the very high or extreme potential dose category (see Section 6.2)

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page 27 of 29		

should be equipped with two independent (redundant) interlocks connected so that either will perform its function in case the other interlock fails,"

NCRP REPORT No. 88, section 4.1, paragraph 5, "Redundancy is necessary despite the use of fail-safe design if the system must function in case of any type of failure."

SLAC 327, section Interlock Design, paragraph 3, "Duplicate (parallel) circuits or redundant components should always be used in critical applications where the single failure of a circuit or device could lead to a hazard. In design of redundant circuits, parallel chains should be used."

Recommendation:
NCRP REPORT No. 88, section 5.2, "Redundancy of components is widely used in the nuclear industry to enhance reliability by increasing the probability that the system will function properly, and to mitigate the effect of failure of key components."

- C.2.5.1.3 The PSS shall have a separate control subsystem for routine operation of beamlines.
- DOE 5480.25 Guidance, Part I.F., section 2. b. (5), " Safety devices should not be used as routine shutdown mechanisms, i.e., the design should provide for an orderly means of turning off beams other than activation of an entry interlock before entry is attempted into a controlled access area."
- DOE 420.2A Guidance, Chapter II, section C. 3. e, " Safety devices should not be used as routine shutdown mechanisms, i.e., the design should provide for an orderly means of turning off beams other than activation of an entry interlock before entry is attempted into a controlled access area."
- NCRP REPORT No. 88, section 3.1.5, paragraph 2, item 5, "Interlocks should not be routinely used to turn off radiation-producing equipment."
- SLAC 327, section Features of an Interlock System, paragraph 4, item 2, "Interlocks are not to be used to shut off beams for routine entries."
- C.2.5.2.1 Each PSS shall be stand-alone and operate on exactly one beamline
- DOE 4580.25 Guidance, Part I.F., section 2. b. (7), "The system could be modular in design so interlocks for different parts of the facility can be serviced independently."
- DOE 420.2A Guidance, Chapter II, section C. 3. g, " The system could be modular in design so interlocks for different parts of the facility can be serviced independently."
- C.2.5.2.2 Where practical, each ESD subsystem shall be programmed by different programmers working independently.
- DOE 5480.25 Guidance, Part I.F., section 2 a.2. (c), "If redundancy is provided by independent computer systems, the logic software for the systems might be written by different programmers, working independently."
- DOE 420.2A Guidance, Chapter II, section C. 2. b. (3), "If redundancy is provided by independent computer systems, different programmers, working independently could write the logic software for the systems."
- C.2.5.3.1 As is reasonable practical, the ESD subsystems shall not perform equipment protection functions.
- ES&H Manual Chapter 5-16 section Hardware Requirements paragraph 4, "Personnel safety systems should be kept separate from the machine components protection systems."
- C.2.5.4.1 Mechanisms shall be provided to allow emergency access and egress.
- DOE 5480.25 Guidance, Part I.F., section 2.c. (2), "Emergency exit mechanisms are required by OSHA standards to be provided at all doors, even when interlocked. Emergency entry features for interlocked door should not be precluded."
- DOE 420.2A Guidance, Chapter II, section C. 4. b., "Emergency exit mechanisms are required by OSHA standards to be provided at all doors, even when interlocked. Emergency entry features for interlocked door should not be precluded."

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>28</u> of <u>29</u>		

ES&H Chap 5-16 Design Req. paragraph 4, "No controls will be installed at any radiological area that would prevent rapid evacuation of personal under emergency conditions.
 SLAC 327, section Features of an Interlock System, item 3, "Emergency exit mechanisms must be provided at all doors and man-ways."

C.2.5.5.1 The safety interlock systems shall not allow program modification while in operation; they must be put in a programming mode via a key.

NCRP REPORT No. 88, section 4.1, paragraph 12, "Also, software and hardware protection mechanisms should be implemented to inhibit accidental or unauthorized alteration of the software."

C.2.5.6.1 The system should be designed such that the ESD portion can be tested independently of the Control subsystem in a non-invasive manner (no signal paths shall be broken).

DOE 5480.25 Guidance, Part 1.F., section 2. b. (8), "The system design should allow for complete function testing, with the effort and disruption required by such tests kept within reasonable limits."

DOE 420.2 Guidance, Chapter II, section C. 3. h., " The system design should allow for complete function testing, with the effort and disruption required by such tests kept within reasonable limits."

SLAC 327, section Interlock Design, paragraph 7, "The equipment design should include ways to manually test the system."

Constraint was internally enhanced to meet major goal for the new system.

C.2.5.6.2 All PSS systems, wiring, and devices must be clearly labeled to note that tampering is strictly forbidden

DOE 4580.25 Guidance, Part 1.F., section 2.b. (6), "A strict configuration control system should protect the circuits and functions against unauthorized and inadvertent modification. Critical devices should be clearly labeled to note that tampering is strictly forbidden."

DOE 420.2 Guidance, Chapter II, section C. 3. f, "A strict configuration control system should protect the circuits and functions against unauthorized and inadvertent modification. Critical devices should be clearly labeled to note that tampering is strictly forbidden."

Recommendation:

SLAC 327, section Electronic Devices, paragraph 3 item 4, "Cable runs for critical devices can be in isolated and/or labeled.

C.2.5.6.3 All PSS circuitry and wiring shall be in secured cabinet, raceways, conduit, or in armored cable not shared with any non-related system.

DOE 5480.25 Guidance, Part 1.F., section 2.b. (3), "System components should be protected from damage, and cable runs outside of cable trays should be armored cable, in conduit, or in flexible conduit.

DOE 420.2A Guidance, Chapter II, section C. 3. c, "System components should be protected from damage, and cable runs outside of cable trays should be armored cable or in conduit."

ES&H Chap 5-16 Hardware Req. paragraph 3, " Safety system components (at a minimum, items such as beam stops, door interlock switches, etc.) should be labeled or color coded and must be secured or supervised to prevent unauthorized access."

NCRP REPORT No. 88, section 4.1, paragraph. 11, "Although it is not always possible to protect logic circuits from deliberate or inadvertent alterations that will preclude proper functioning, every reasonable effort should be made to prevent such alterations." and section 5.4, "In addition to being protected against natural environmental conditions alarm and access control system should also be protected against deliberate or accidental intrusion. ... Tamper resistance can take many

	ARGONNE NATIONAL LABORATORY	Document No. 4104013001-00017		
	Title: System Requirements Specification	Rev. 00	Approved	Date 03/10/2004
	Generation-3 Personnel Safety System	Page <u>29</u> of <u>29</u>		

forms, ranging from simply placing equipment in locations that are nor easily accessible, such as high up on a wall, to isolating the system within a lock enclosure."
 SLAC 327, section Interlock Design, paragraph.5, "To reduce the likelihood of accidental damage or deliberate tampering, all cables should be protected." and paragraph 6, "Logic equipment should be mounted in locked racks, cabinets or boxes." and section Electronic Devices, paragraph 3 item 2, "Critical electronics can be locked in cabinets." and item 4, "Cable runs for critical devices can be in isolated and/or labeled.

C.2.5.6.4 Crash Buttons shall be clearly visible and unambiguously labeled

DOE 5480.25 Guidance, Part 1.F., section 2.c. (1), "Emergency shut-off devices, which are clearly visible, unambiguously labeled and readily accessible, should be provided in exclusion areas."

DOE 420.2 Guidance, Chapter II, section C. 4. a., "Emergency shut-off devices, which are clearly visible, unambiguously labeled and readily accessible, should be provided in exclusion areas."

ES&H Chap 5-16 Design Req. paragraph 2, "Emergency shut-off devices (scram switches) that are clearly visible, unambiguously labeled, and readily accessible should be provided by the facility manager, even when interlocks are not required." and section Hardware Req., paragraph 10, " A scram switch, pull-chain, or other emergency power cutoff switch shall be clearly visible, unambiguously labeled, and located within easy reach.

SLAC 327, section Features of an Interlock System, item 1, "Emergency-off (Scram) buttons should be clearly visible, labeled and readily accessible."

C.2.5.7.1 Crash buttons shall require manual resetting.

ES&H Chap 5-16 Hardware Req. paragraph. 10, "Such a cutoff switch should have positive indication of the operative position of the switch and should include at the same location, a manual reset so that the accelerator cannot be restarted from the radiation-generating device control console without manually resetting the cutoff switch.

C.2.5.7.2 Door closed sensor shall be inaccessible for the outside of the enclosure.

ES&H Chap 5-16,section Hardware Req., paragraph 4, "There must be two redundant methods monitoring each personnel access point that are not subject to a common mode failure (for example, one pulsed optical sensor set, or one mechanical and one magnetic switch, or two independent mechanical switches). The switches or sensors shall be inaccessible from the "safe" side of the access point."