National Spherical Torus eXperiment Upgrade

NSTX-U Personnel Safety System-Safety Instrumented Systems Requirements

NSTX-U-RQMT-RD-024-02

November 25, 2019

Stefan Gerhardt
Digitally signed by Stefan Gerhardt
Date: 2019.11.25 20:31:16 -05'00'

Prepared by: Stefan Gerhardt , Systems Engineering and Integration

Peter Dugan
Digitally signed by Peter Dugan
Date: 2019.11.26 08:20:41 -05'00'

Reviewed by: Peter Dugan, Systems Engineering and Integration

Timothy N. Stevenson
Digitally signed by Timothy N. Stevenson
Date: 2019.11.26 09:39:31 -05'00'

Reviewed By: Tim Stevenson, NSTX-U Operations Head, OSS RE

Joseph R_ Petrella Jr_
Digitally signed by Joseph R_ Petrella Jr_
DN: C=US, O=PPPL, CN=Joseph R_ Petrella Jr_, E=jpetrell@pppl.gov
Reason: I have reviewed this document
Location:
Date: 2019-11-26 10:25:05

Reviewed by: Joseph Petrella, Project Cognizant Engineer

PAUL SICHTA
Digitally signed by PAUL SICHTA
Date: 2019.11.26 14:39:26 -05'00'

Reviewed by: Paul Sichta, Control and Data TA

Yuhu Zhai
Digitally signed by Yuhu Zhai
Date: 2019.11.27 13:42:59 -05'00'

Approved By: Y. Zhai, NSTX-U Project Engineer

Record of Revisions

Date	Version	Brief Description of Changes
12/5/18	Rev 0	Initial Release
6/12/19	Rev 1	Major revisions moving from CDR to PDR stage; all sections touched.
11/25/19	Rev 2	Replace “LOCKED” with “LOCKDOWN”
		Updated section 3.2 to accommodate revised interdiction device strategy
		Significant modifications to section 3.8.2 to accommodate revised strategies on the exclusion area HMI.
		Added new sections 3.18 and 1.19
		Updated Table 3.6-1.

References

[1] NSTX-U-RQMT-GRD-001, NSTX-U General Requirements Document

[2] NSTX-U-RQMT-SRD-012, NSTX-U SRD – Operations and Safety Systems

[3] ASO-180529-SPG-01, PRELIMINARY CONCLUSIONS REGARDING THE PROCESS AND FORMAT OF RISK ANALYSIS IN THE NSTX-U SAD

[4] OPS-181205-JM-01, Hazard Analysis for the Personnel Safety Systems (PSS) CDR

[5] NSTX-U-RQMT-RD-026, NSTX-U Trapped Key System Requirements

[6] NSTX-U-RQMT-RD-027, NSTX-U Configuration Controlled Safeguards Requirements

1: Scope

a. This document provides implementation requirements for the NSTX-U Personnel Safety System Safety Instrumented System

b. General requirements for the system are provided in the NSTX-U General Requirements Document [1].

c. System requirements are provided in Operations and Safety Systems System Requirements Document [2]. This document flows the system requirements in that SRD down to specific implementation requirements.

2: Definitions

Definitions relevant to this RD are provided in the Ref. [2].

3: Design Requirements

3.1: Hazard Analysis and SIS SIFs

a. A hazard analysis shall be performed to identify hazardous conditions that require credited controls.
b. The hazard analysis shall identify the severity and likelihood of unmitigated risks as described in Refs. [3,4] .
c. Each hazard identified by the analysis shall be mitigated by existing laboratory safety program(s), a PSS-SIS function, some other NSTX-U related safety system, or a combination thereof.
d. Safety Instrumented Function(s) requirements shall be developed from a Layer Of Protection Analysis to establish the need for residual risk mitigation by a Safety Instrumented System.
e. Target Risk Reduction Factors shall be assigned to each Safety Instrumented Function based on the highest residual risk identified in the analysis that is mitigated by that Safety Instrumented Function.

3.2 PSS-SIS Interlocked systems

a. The PSS-SIS Interlocked Systems shall include those identified in Ref. [2], as are the general actions PSS-SIS will take in the event the CCS/BCS has failed to render interlocked equipment safe upon a PSS-SIS Emergency Stop as described in section 3.1 of Ref. [2].

b. In the event of PSS-SIS interdiction upon an PSS-SIS Emergency Stop, the neutral beam system interdicted devices shall respond as per Table 3.2-1

***Table 3.2-1**: Required response of the PSS-SIS Interlocked Devices to render the Neutral Beam System safe after a PSS-SIS Emergency Stop*

1	Open the SV bus breakers that feed the acceleration power supplies (transformer rectifiers and modulator-regulator tubes) (ESV2-SB10, -SB11)
2	Open the SF bus breaker that feed the acceleration power supplies (transformer rectifiers and modulator-regulator tubes) (ESF1-SB10)
3	Open the SF bus breaker that provide pulsed power for the arc and filament power supplies (ESF2-SB05)

c. In the event of PSS-SIS interdiction upon an PSS-SIS Emergency Stop, the FCPC interdicted devices shall respond as per Table 3.2-2

***Table 3.2-2**: Required response of the PSS-SIS Interlocked Devices to render the FCPC System safe after a PSS-SIS Emergency Stop*

1	Open the SV bus breakers that feed the FCPC rectifiers with appropriate time delay (e.g. ESV1-SB01)

d. Additionally, the actions in Table 3.2-3 shall be taken.

***Table 3.2-3**: Additional actions in the event of a PSS-SIS Emergency Stop*

1	If the actions described in Tables 3.2-1 and 3.2-2 are not completely successful, open the breaker ESF1-SB01 (S1-B1) that feeds D-site experimental power.

e. The PSS-SIS shall have the ability to detect inconsistent states of equipment as an additional action. The ability to do this shall include the capabilities described in Table 3.2-4.

***Table 3.2-4**: Diagnostic capabilities required for the detection of an inconsistent state.*

1	Monitor the position of all breakers in Table 3.2-1
2	Monitor the position of all breakers in Table 3.2-2
3	Monitor the position of breakers in Table 3.2-3
4	Monitor the position of TF line and ground switches
5	Monitor the position of OH line and ground switches
6	Monitor the position of the PF line and ground switches
7	Monitor the position of PCTS links
8	Monitor the position of Neutral Beam Ross grounding switches
9	Monitor the position of the Neutral Beam Pringle grounding switches
10	Monitor the position of the PCTS guard trapped key
11	Monitor the position of the ESF2-SB05 trapped key

f. The CCS/BCS performs a controlled shutdown of Interlocked Devices immediately upon PSS-SIS revoking permissives to CCS/BCS. PSS-SIS is not required to interdict interlocked devices if CCS/BCS successfully renders safe at a minimum one logical element of each Interdicted Device within the allotted 1-½ seconds.

3.3 Access Control

3.3.1 Exclusion Areas

a. The PSS-SIS shall facilitate establishing and maintaining exclusion areas.
b. The PSS-SIS exclusion areas are identified in Ref. [2].

3.3.2 Access Control Requirements

a. The PSS-SIS shall monitor the status of entryways, movable shielding, and other accessways that allow access to securable areas.
b. Access to a securable area shall be inhibited[1] and monitored while the securable area is in NO ACCESS state.
c. The PSS-SIS shall have features to ensure that PSS-SIS interlocked devices are prevented from delivering hazards into the exclusion area when the area is safe for personnel occupancy (see Section 3.19)
d. The PSS-SIS shall provide clearly visible status indicators of the “Safe” or “Unsafe” status for each of the securable areas (See Section 3.8 below).
e. The PSS-SIS shall provide an audible and visual warning before transitioning from a “Safe” mode to an “Unsafe” mode. (See Section 3.8 below)

Note: An administrative announcement over a public address system may substitute for an automated audible warning if it is preceded by a klaxon/horn warning.

[1] Inhibit: e.g. locally disable ACAMS access to the exclusion area

f. The PSS-SIS shall provide clearly visible status or warning indicators outside of each entrance to a securable area. The status indicators shall be an indication of the safe or unsafe mode within that area.

g. When the unsafe status in any securable area is pending, audible warnings must be broadcast within the securable area.

h. The system shall accommodate the use of the ACAMS card reader for use during ACCESS state to regulate access to designated areas.

i. The ACAMS door card reader shall not degrade any Safety Instrumented Functions or PSS-SIS Additional Actions.

j. The system shall disable the functionality of the ACAMS door card readers for securable areas when in NO ACCESS.

k. The PSS-SIS shall use diverse components where practical when redundant input or output devices are used.

3.3.3 Search and Secure

a. The establishment of an exclusion area shall require a visual search and secure (sweep) of the area.

b. The search and secure pattern when required in complex spaces shall follow a designated pattern designed to ensure all regions in securable areas are observed.

c. The activation of Search and Secure stations in the improper order shall require the search be restarted.

d. An access violation during the execution of the search and secure process in a complex space shall require the search be restarted.

e. Dropping the loop in one securable area shall not require that the loops in other unconnected securable areas be dropped.

f. The system shall disable the functionality of the ACAMS door card readers, if equipped, for securable areas when conducting a Search and Secure.

3.4 PSS E-STOP Buttons

a. PSS-SIS E-STOP buttons shall be provided inside securable areas, and one immediately outside an entrance to a securable area.

b. PSS-SIS E-STOP buttons within securable areas shall be placed such that no accessible area is more than 50 ft from a button

c. PSS-SIS E-STOP buttons shall have a latching feature and require a local physical reset before a system reset can be performed.

3.5 Interlock Requirements

a. The conditions for declaring a PSS-SIS Emergency Stop are provided in Ref. [2].

b. The actions to take following a PSS-SIS Emergency Stop are provided in Ref. [2].

c. The PSS-SIS design shall achieve the required risk reduction as required by associated Safety Instrumented Function(s).

d. Dual chain architecture shall be implemented and each chain shall extend from sensors to final devices.

e. The signal path between the processing elements of the PSS-SIS and the devices which remove hazards in a shutdown situation shall have a minimum number of intermediate components.

f. PSS-SIS equipment and wiring shall be located in dedicated PSS-SIS racks.

g. All PSS-SIS functions shall be resilient against single chain undetected failures.

h. 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 PSS-SIS.

i. The PSS-SIS shall not be used to provide the normal on/off control of a PSS-SIS interlocked device.

j. The PSS-SIS shall not automatically reset once a tripped interlock is restored. A manual reset by a qualified operator shall be required.

k. The PSS-SIS shall have the ability to monitor the status of interdiction devices for interlocked equipment w/o reliance on the CCS.

Note: Exception may be granted in a future case that a portion of the CCS is certified with the appropriate SIL rating.

l. The PSS-SIS logic solver shall be immune to unresponsive modes by defaulting to a safe condition.

m. The PSS-SIS logic solver shall be immune to error modes by defaulting to a safe condition.

3.6 States of Operation and Inconsistent Configurations

a. The PSS-SIS states for a securable area shall be individually classified as "ACCESS", "NO ACCESS", and “LOCKDOWN”.

b. When in ACCESS, at a minimum a single logical element of each PSS-SIS monitored device shall be in a safe mode.

c. Inconsistent configurations when in ACCESS shall include those in Table 3.6-1.

***Table 3.6-1**: Inconsistent configurations when in ACCESS state.*

1	Any FCPC line switch closed if the corresponding breakers are closed if not configured for dummy load testing
2	Any FCPC ground switch open if the corresponding line switches or breakers are closed if not configured for dummy load testing
3	ESF1-SB10 or ESV2-SB10 or ESV2-SB11 NB high voltage breakers are closed *AND* paired NB Pringle and Ross Switch are not closed *AND* ESF2-SB05 is closed

d. Inconsistent configurations when in any state shall include those in Table 3.6-2.

***Table 3.6-2**: Inconsistent configurations when in any state.*

1	ESF2-SB05 trapped key position is inconsistent with the breaker position when the breaker is closed
2	PCTS guard trapped key position is inconsistent with the PCTS bus link monitor if the PCTS guard is in place
3	A breaker remains closed when it is being commanded to be open
4	An interdiction relay commanded position and feedback is inconsistent

3.7 Design Features for Testing

3.7.1 Interlocked Equipment Testing

a. The PSS-SIS shall have capabilities that accommodate specific test modes of PSS-SIS interlocked equipment. Examples of such test modes include those in Table 3.7-1.

***Table 3.7.1-1**: Interlocked Equipment Test Modes*

1	FCPC open circuit testing
2	FCPC rectifier dummy load testing
3	Neutral beam modulator/regulator testing

3.7.2 PSS-SIS Testing

a. Designed features of the PSS-SIS shall facilitate testing of the system to ensure the Safety Instrumented Functions are properly implemented.

3.8 Human Machine Interface

There are two types of PSS-SIS Human Machine interfaces: Centralized and those that are at or within exclusion areas

3.8.1 Centralized HMI

a. The centralized HMI for the PSS-SIS (PSS-CHMI) shall be located at the station for the Chief Operating Engineer in the NSTX-U Control Room.

b. The PSS-CHMI shall provide means for the operator to authenticate (e.g. password, physical device such as token or key).

c. The PSS-CHMI shall provide a mechanism i.e., key to ensure that only the authorized individual can access and change permissive status using the PSS-CHMI.

d. The PSS-CHMI shall indicate the access state of each securable area (ACCESS, NO ACCESS, LOCKDOWN).

e. The PSS-CHMI shall indicate the interlock status is complete and ready to permit machine operation.

f. The PSS-CHMI shall indicate that when exclusion areas are secured.

Note: this provides an indication that exclusion areas are cleared of personnel

g. The PSS-CHMI shall indicate whether a ESTOP button has been depressed and its identity/location.

h. The PSS-CHMI shall indicate for each securable area whether a door violation has occurred. It may additionally indicate which door had the violation if there is more than one door to the area.

i. The PSS-CHMI shall indicate the "safe" status of each PSS-SIS interlocked device.

j. The PSS-CHMI shall have a physical PSS-SIS E-STOP button that functions equivalently to an ESTOP button within a securable area.

k. The PSS-CHMI shall display the fault status of the PSS-SIS.

l. The PSS-CHMI shall have the capability to reset an NSTX-U E-STOP after a local physical reset IF REQUIRED (per section 3.4)

m. Restoration of the PSS-SIS system after an E-STOP event shall be achieved through the COE coordinating the resetting the field device as well as the execution of dedicated E-STOP restoration procedures.

n. The local lamp test of the PLC controlled status lamps should be controlled via the PSS-CHMI.

o. The Emergency Egress status of each TKS personnel access door so equipped shall be displayed in the PSS-CHMI.

3.8.2 HMI At and Within Exclusion Areas

a. The HMI outside each door to a securable area shall indicate the safe or unsafe status of its area.

b. The HMI outside of one door to each complex securable area shall indicate the status of the search and secure status and provide functionality required to support the Search and Secure.

c. Audible and visual alerts or other mechanisms inside of securable areas shall be used to indicate a pending transition to an unsafe mode.

3.9 Tamper Resistance and Labeling

a. Conduits associated with the PSS-SIS shall be clearly identified.

b. Junction boxes containing PSS-SIS electronics shall have labels indicating that the system is used for PSS and must not be modified unless authorized.

c. The PSS-SIS shall employ deterrents to prevent and discourage physical tampering or alteration of hardware components.

d. Methods shall be used to hinder or detect tampering.

e. Features shall prevent the operation of interlocked devices when a tamper-detecting cover to a PSS-SIS logic solver, network rack(s), or it's IO enclosure(s) is disturbed.

f. A log/audit trail of tampering shall be maintained.

g. The PSS-SIS shall monitor and annunciate inputs for inconsistent modes that indicate an unauthorized configuration change.

h. Authorized changes to the PSS-SIS hardware, settings, or software shall only occur during a verified safe mode.

3.10 Logging

a. The status of critical PSS-SIS I/O shall be logged.

b. The PSS-SIS access state of each area shall be logged.

c. The archival shall be at a rate consistent with the use case of the data.

d. Storage capacity shall permit at least a full month of data to be stored, with the oldest data being overwritten first.

e. It shall be possible to archive some portion of the logged data for arbitrary duration.

Note: This mode may be used to ensure, for instance, that data being used to understand an event is retained beyond the standard archival window.

f. The time used for Log-message timestamps for PSS-SIS and CCS shall be capable of being correlated if logging is a feature of the CCS.

3.11 Cyber Security

a. PSS-SIS computing assets shall not communicate on corporate or other control system networks.

b. A software version control process shall be utilized in the development of this system's software.

c. Communication between elements of the PSS shall utilize protocols that are inherently secure.

d. Access to the PSS-SIS (other than the dedicated operator HMIs) shall originate from a computer that: requires multi-factor user authentication, has up-to-date security patches, and is PPPL supplied and managed.

e. Access to PSS-SIS equipment shall be prevented by physical and/or electronic barriers to prevent tampering by unauthorized personnel.

f. User roles shall be established, assigning privileges to specific roles for which they are required as determined by the system owner.

g. The PSS-SIS documentation shall include policies, procedures and training material necessary for secure operation by qualified individuals.

h. All unused communication ports and services on PSS-SIS equipment shall be disabled. This includes both hardware and software.

i. Vendors selected for Hardware and Software supply shall be confirmed as authorized resellers by manufacturer.

j. Comply with PPPL Standard Cyber Security Program Plan (CSPP) with anticipating 800-53r4 controls at the moderate level. Risk management shall be utilized to evaluate deviations with approval of the system owner.

k. Records to be kept include those in Table 3.11-1.

***Table 3.11-1**: Records related to cybersecurity*

1	Those who have physical access to these systems to perform maintenance
2	What maintenance task(s) are performed
3	When these tasks are performed.

l. The development environment, system firmware, system diagnostic data and configuration shall be archived periodically. Each archive shall be verified once stored.

m. Access to the system for maintenance and monitoring activities shall not create a bridge between PSS network and any other network.

3.12 Modifications

a. Permanent modifications to installed PSS-SIS systems shall be reviewed via the engineering design review process and be accompanied by a USI determination.

b. Changes to PSS-SIS interlocks shall require recertification of the interlock and PSS-SIS equipment and functions that are associated with the interlock using approved test procedures per ENG-030.

c. Temporary modifications to the PSS-SIS shall follow the T-MOD process outlines in ENG-036. As per that procedure, a USID is required for any T-MOD to the PSS.

3.13 Expansion

a. Provision shall be made for the addition of new Interlocked equipment.

b. Provision shall be made for the addition of new Exclusion Areas.

c. Provision shall be made for the addition of ESTOP buttons in and outside of existing or new exclusion areas.

d. Provision shall be made for additional types of access states.

e. Provision to introduce additional external inputs to the PSS-SIS in order to trigger response shall be provided.

Example: the ability to trigger a transition to the NTC "LOCKDOWN" state based on a signal from the NSTX-U ODH system.

3.14 Design, Installation, & Commissioning

a. Reviews for the PSS-SIS system shall involve subject matter experts external to PPPL.

b. All PSS-SIS equipment shall be installed by personnel approved by the NSTX-U Head of Operations

c. The PSS-SIS pre-operational testing shall follow one or more written procedures. These procedures shall be reviewed and approved by the NSTX-U Head of Operations, in addition to the reviews and approvals mandated in ENG-030 *PPPL Technical Procedures*.

d. Installation and pre-operational testing activities shall include the activities in Table 3.14-1:

Table 3.14-1: Installation and pre-operational testing activities

1	Inspection of proper connection of grounding and power
2	Verification of expected power loading coming into cabinets
3	Inspection for physical damage
4	Proper calibration of PSS-SIS inputs and outputs
5	Verification of PSS-SIS logic solver operation
6	Verification of software versions used (if applicable)
7	Verification of PSS-SIS inputs and outputs
8	Verification of interfaces to non-PSS equipment

e. The PSS-SIS validation procedure shall follow a written Integrated System Test Procedure.

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 into an overall certification procedure

f. PSS-SIS validation shall include static and functional tests of all PSS inputs, outputs, and operational modes

g. As part of the installation process, all abandoned access control hardware associated with exclusion areas shall be removed.

h. Any access control equipment that is abandoned in place shall be clearly and permanently labelled as being out of service.

i. Any software developed for the PSS shall implement the PPPL Software QA procedures, as appropriate.

3.15 Certification & Maintenance

a. PSS-SIS Systems shall undergo periodic certification (proof testing) as required by the system design (e.g. SIL), regulatory requirements, or laboratory policy (whichever is shortest).

b. Problems found during certification shall be repaired and retested before operations are allowed.

c. Certification procedures shall include static and functional tests of all PSS-SIS inputs, outputs, and operational modes.

d. Certifications shall extend from the sensor to the final element.

e. Records of completed certifications shall be maintained by the Operations Center

f. Each PSS-SIS system shall undergo periodic maintenance required to demonstrate the designed risk reduction capability

g. Only personnel approved by the NSTX-U Operations Head shall be authorized to work on PSS-SIS devices or wiring

h. Operations shall be suspended before any work on a PSS-SIS device or component starts

i. Operations shall be suspended in any area where a PSS-SIS device is suspected of being defective. Operations may not resume until the device is repaired and recertified or it is determined by Operations Group personnel that the device is functioning as designed; the Operations Group Head must concur with this finding.

3.16 Interfaces

See interface tables in Ref. [2]

3.17 Codes and Standards

See codes and standards in Ref. [2]

3.18 Interactions with the Trapped Key System

a. The status of the key blocks in table 3.18-1 shall be made available to the PSS-SIS.

Table 3.18-1: Key blocks whose status shall be monitored by the PSS-SIS

PCTS Dummy Load Guard Key
NB Dummy Load Interlock Key
NSTX-U NTC North Door S&S Key
MER Mezzanine Door S&S Key
NSTX-U NTC North Door Vestibule Key
MER Mezzanine Door Vestibule Key

b.The Emergency Egress status of each TKS personnel access door so equipped shall be monitored by the PSS-SIS.

Table 3.18-2: TKS Emergency Egress Pushbuttons whose status shall be monitored by the PSS-SIS

NSTX-U NTC North Door Vestibule
NSTX-U NTC South Door Vestibule
MER Mezzanine Door Vestibule
Cable Spread Room entryways
TCB cage entryways

3.19: Interactions with the Centralized Control System (CCS)

a. The CCS interface to the PSS-SIS shall not degrade the safety capability of the PSS-SIS.
b. Communication between the PSS-SIS and the CCS shall be electrically isolated for control signal levels.
c. The PSS-SIS shall provide a PSS-SIS Emergency Stop signal to the CSS.
d. The PSS-SIS shall provide a "safe to Enable FCPC" signal after a 300 second delay to the CCS based on the criteria in Table 3.19-1

Table 3.19-1: Criteria for sending the "safe to Enable FCPC" signal

For Dummy Load Testing: PTCS Dummy Load Guard Present + No PCTS Bus Link Present + NO ACCESS state for TCB Cage Area + NO ACCESS state for Cable Spread Room
-----OR------
For Coil Operations: NO ACCESS state for NTC + NO ACCESS state for MER Mezzanine + NO ACCESS state for TCB Cage Area + NO ACCESS state for Cable Spread Room

e. The PSS-SIS shall provide a "safe to Enable NB" signal after a 300 second delay to the CCS based on the criteria in Table 3.19-2

Table 3.19-2: Criteria for sending the "safe to Enable NB" signal

For Dummy Load Testing: NB Dummy Load Configured with Trapped Key + ESF2-SB05 OPEN Position
-----OR-----
For Beam Acceleration Operations: NO ACCESS state for NTC + NO ACCESS state for MER Mezzanine

f. The PSS-SIS shall provide the area status (ACCESS, S&S in progress, NO ACCESS, LOCKDOWN) to the CCS for the following areas:
    i. NSTX-U Test Cell
    ii. MER Mezzanine

g. The PSS-SIS shall provide the area status (ACCESS, NO ACCESS, LOCKDOWN) to the CCS for the following areas:
    i. Test Cell Basement Cage Area
    ii. Cable Spread Room
h. The PSS-SIS shall send an “SIS alarm” signal to the CCS indicating alarms other than an NSTX-U PSS-SIS Emergency Stop.
i. The PSS-SIS shall send a configuration signal to the CCS indicating the dummy load configuration for:
    i. FCPC (see Table 3.19-1)
    ii. NB (see Table 3.19-2)