National Spherical Torus eXperiment Upgrade

National Spherical Torus Experiment-Upgrade

NSTX-U

SYSTEM REQUIREMENTS DOCUMENT

Operations and Safety Systems

NSTX-U-RQMT-SRD-012-02

November 25, 2019

Stefan Gerhardt Digitally signed by Stefan Gerhardt Date: 2019.11.25 20:29:49 -05'00'

Prepared By: Stefan Gerhardt, Systems Engineering and Integration

Peter Dugan Digitally signed by Peter Dugan Date: 2019.11.26 08:19:46 -05'00'

Reviewed By: Peter Dugan, Systems Engineering and Integration

Timothy N. Stevenson Digitally signed by Timothy N. Stevenson Date: 2019.11.26 09:38:12 -05'00'

Reviewed By: Tim Stevenson, NSTX-U Operations Head, OSS, NTC, and Heating Systems RE

Yuhu Zhai Digitally signed by Yuhu Zhai Date: 2019.11.26 11:07:17 -05'00'

Reviewed By: Yuhu Zhai, NSTX-U Project Engineer

Leslie Hill Digitally signed by Leslie Hill Date: 2019.11.27 07:56:58 -05'00'

Reviewed By: L. Hill, NSTX-U Project Manager

William V. Slavin Digitally signed by William V. Slavin Date: 2019.12.02 08:52:36 -05'00'

Reviewed By: William Slavin, Industrial Hygiene and Safety TA

PAUL SICHTA Digitally signed by PAUL SICHTA Date: 2019.12.02 09:42:48 -05'00'

Reviewed By: Paul Sichta, Control and Data TA

GEORGE ASCIONE Digitally signed by GEORGE ASCIONE Date: 2019.12.02 12:28:11 -05'00'

Reviewed By: George Ascione, Radiation Protection TA

National Spherical Torus eXperiment Upgrade

Raymond A. Camp
Digitally signed by Raymond A. Camp
DN: cn=Raymond A. Camp, o=PPPL, ou=Power Systems Group, email=rcamp@pppl.gov, c=US
Date: 2019.12.04 13:43:44 -05'00'

Reviewed By: Ray Camp, Electrical TA

Robert Ellis
Digitally signed by Robert Ellis
Date: 2019.12.04 17:27:08 -05'00'

Approved By: R. Ellis, PPPL Chief Engineer

John N. Galayda
Digitally signed by John N. Galayda
Date: 2019.12.05 08:12:48 -05'00'

Accepted by: J. Galayda, NSTX-U Project Director

Change Record

Rev.	Date	Description of Change
0	12/5/18	Initial Release; note that the section on the radiation monitors was directly transferred from NSTX-U-RQMT-SRD-010-01, and the sections on the PSS-SIS and CCS replace the HIS section of NSTX-U-RQMT-SRD-010-01. The section on the test cell ODH monitor is transferred from NSTX-U-RQMT-RD-006-00.
1	6/12/19	Added new Section 4 for the trapped key system, and new Section 5 for the Configuration Managed Safeguards
		Major updates to PSS-SIS requirements in Section 3, updating from CDR requirements to PDR requirements
		Update definitions in Section 2
		Updated CCS interface table
2	11/25/19	Updated the locations of ODH monitors, as per memo OSS-191022-SPG-01
		Updated Section 9.2 to require the ODH system design be guided by ISA–RP92.04.02, Part II–1996 (R2013)
		Changed “LOCKED” to “LOCKDOWN”, & clarified definition in table.
		Updated 3.2.2d
		Updated 3.3d
		Updated definition of “PSS-SIS Emergency Stop” in table of definitions
		Adjustment of text in Table 3.3-4.
		Updated section 6.3 & 6.5
		Updated Table 3.3-4
		Updated Table 3.1.1.1-1
		Added Table 3.1.1.2-1 indicating additional areas under access control
		Updated Table 3.3-2.
		Removed requirement for an audible alarm on the NTC ground fault monitor.

Table of Contents

References

[1] NSTX-U-RQMT-GRD-001, NSTX-U General Requirements Document
[2] NSTX-U Personnel Safety System Requirements, NSTX-U-RQMT-RD-024-00
[3] OPS-181205-JM-01, Hazard Analysis for the Personnel Safety Systems (PSS) CDR
[4] DOE O 420.2C, *Safety of Accelerator Facilities*
[5] DOE G 420.2-1A, *Accelerator Facility Safety Implementation Guide for DOE O 420.2C, Safety of Accelerator Facilities*
[6] 10 CFR 835, *Occupational Radiation Protection Program*
[7] 10 CFR 851, *Worker Safety and Health Program*
[8] PPPL Environment, Safety, and Health Directives ESHD 5008, *PPPL Safety Manual*
[9] IEC 61511, *Functional Safety - Safety instrumented systems for the process industry secto*r
[10] NSTX-U-DOC-112-00, NSTX-U Preliminary Hazard Analysis Report
[11] NSTX-U Centralized Control System Requirements, NSTX-U-RQMT-RD-025-00
[12] NSTX-U Trapped Key System Requirements, NSTX-U-RQMT-RD-026-00
[13] NSTX-U Configuration Controlled Safeguard Requirements, NSTX-U-RQMT-RD-027-00
[14] Safety Assessment Document (SAD),NSTX-U-SAD-001-00
[15] Hazard Analysis Report (HAR), NSTX-U-DOC-123-00
[16] Interlock Key Control, ENG-011
[17] PPPL Standard Cyber Security Program Plan, CSPP
[18] Software Quality Assurance, QA-028

1.0 Scope

a. The scope of the document addresses the Operations and Safety Systems consisting of the Personnel Safety System, the Centralized Control System, the Ground Fault Monitoring System, the Area Radiation Monitors, and the Oxygen Deficiency Monitor.

b. The format of this document, including interfaces specifications, is provided in the General Requirements Document [1].

2.0 Definitions & Assumptions

Table 2.0-1: *Definitions*

Acronym or Abbreviation	Term	New Description
	ACCESS	A state where access to exclusion areas is unrestricted, except possibly by the PPPL card reader systems in select cases (this is referred to as Administratively Controlled Access). Each exclusion area can independently be configured for this state.
	Additional Actions & Functions	Actions and Functions performed by the PSS-SIS that are not required to be included in Safety Instrumented Functions.
ACAMS	Access Control and Alarm Monitoring System	The system that, among other functions, provides card readers on doors at PPPL in order to provide access control to areas. ACAMS may not be used to implement any safety function required for the PSS-SIS.
	access state	The access state describes the various states of any securable area, e.g. ACCESS, NO ACCESS.
	Assumption Identifier	A unique identifier assigned to each assumption made in the implementation of the PSS
	Armed	A mode of a sub-system where primary power is applied such that a timing signal can pulse the system, transferring energy to the experimental areas or dummy loads.
ASE	Accelerator Safety Envelope	As per DOE G 420.2-1a, the accelerator safety envelope is "a set of verifiable physical and administrative credited controls that define the bounding conditions for safe operation and address the accelerator facility hazards and risks."
ASO	Accelerator Safety Order	DOE O 420.2c *Safety of Accelerator Facilities* is known as the ASO. It was added to PPPLs contract in 2016.
	Bakeout Mode	A specific mode where the medium temperature water system, the CS DC supply, and the hot helium system are used to heat the vacuum vessel and components internal to the vessel.
BCS	Basic Control System	The control system for some piece of equipment providing operator interface and control capability. Basic control systems are not designed to the standards of Safety Instrumented Systems.
CCS	Centralized Control System	The centralized control system provides functions that are related to the operation of equipment but are not credited with removing hazards for Interlocked device. Controlled equipment may receive operating permissives from the CCS.
CHMI	CCS HMI	A centralized HMI for the CCS. This is located in the control room.
	Card Reader Access	Access to some areas is restricted by card readers even in ACCESS state; this is utilized to ensure that accessors have proper training, and as a means of property control. The card readers are not used for implementation of PSS-SIS safety functions.
	certification	The final end-to-end testing of the PSS-SIS, providing validation that the system is ready to support safe NSTX-U operations. Validation is done via an ISTP for the system and is repeated on a periodic basis or after significant changes to the system.
	Complex Space	In the context of search and secure, a complex space is one where inspection from a single location is insufficient to establish the space is not occupied.
	Controlled Equipment	This class of equipment is any device whose disabled/disarmed status or permissive is controlled using the CCS. These devices may additionally be Interlocked if they meet additional criteria.

	Disabled	A mode of a sub-system where primary power is removed from the system.
	Disarmed	A mode of a sub-system where the timing signals are not capable resulting in the sub-system creating a hazard in exclusion areas.
DNB	Diagnostic Neutral Beam	A small neutral beam, which when injected into the plasma, produces light which is interrogated to diagnose characteristics of the plasma.
	Direct Ionizing Radiation	Ionizing radiation are those forms of radiation (alpha, beta, gamma, neutrons, ...) capable of producing ions when they interact with matter. Ionizing radiation is much more energetic than non-ionizing radiation such as microwaves. Direct Ionizing Radiation refers to Ionizing Radiation produced by the NSTX-U pulse or neutral beam injection into calorimeters..
	Door Violation	A door violation occurs when any monitored door (personnel door, mobile shield door) is opened after a securable area has had its loop set.
	Dummy load	A device used to mimic the electrical properties of the test cell device for the purpose of testing e.g. NSTX-U Coils, RF antennas, Neutral Beam Ion Source.
ECH	Electron Cyclotron Heating	Electron cyclotron waves are waves with a frequency that is a low harmonic of the electron cyclotron frequency. Waves launched at this frequency can be used to create plasma, heat plasma, or drive currents in the plasma. On NSTX-U, a short pulse (~ 20 msec typically, up to 100 ms max) klystron with up to 30 kW of power and a frequency of 18 GHz is used to assist in the breakdown of the plasma at the beginning of the discharge.
	PSS-SIS Emergency Stop	This is a manual or automatic command which will cause all PSS-SIS interlocked subsystems to revert to a safe condition (shutdown) after an allowed delay to allow existing control systems to perform controlled transitions to a safe state (shutdown).
E-STOP	Emergency Stop Push Button	These units will be placed within specific Exclusion areas, outside of specific Exclusion areas and in the NSTX-U Control Room. Their purpose is to initiate a PSS-SIS Emergency Stop. If one of these buttons is operated, it must be manually reset and acknowledged by the COE before the PSS-SIS Emergency Stop can be cancelled. *Note: individual subsystems may have their own local e-stop buttons - these are not a part of the PSS-SIS.*
	Enabled	A mode of a sub-system with primary power applied (i.e. breakers or contactors closed), but no ability to transfer hazardous energy to exclusion areas or dummy load.
	Exclusion Area	Any area to which access is controlled to prevent the exposure of personnel or the public to hazards.
	Experimental Areas	The exclusion areas for NSTX-U. These include the NTC, the MER, the cable spread room, etc.
	Experimental Complex	All of PPPL D-site (except the tritium areas), and C-site portions of PPPL that support NSTX-U operations (the control room and the RF areas).
	Fault	A condition of the PSS-SIS components that exists which prevents the PSS-SIS from operating
	facility operations	The complete set of tasks required to maintain and operate NSTX-U. This can include maintenance tasks on the various parts of the infrastructure, upgrades and installation of new components and capabilities, pre-operational and integrated testing, and the operation of equipment to support NSTX-U engineering and research operations.
FCPC	Field Coil Power Conversion	The part of the NSTX-U infrastructure containing the rectifiers and inverters used to power NSTX-U coils.
GDC	Glow Discharge Cleaning	Glow discharge cleaning is a means by which a low temperature DC plasma is introduced to the NSTX-U vacuum vessel, with the intent of cleaning the inner surfaces by physical and potentially chemical sputtering. This plasma is formed by electrodes mounted inside the vessel, which are biased to up to 1 kV.
HHFW	High Harmonic Fast Wave	High Harmonic Fast Waves are a type of plasma wave, with a frequency that is a high (10x) harmonic of the ion cyclotron frequency. The system of RF transmitters, transmission lines, and antennas used to launch high-harmonic fast waves is referred to as the HHFW system. The HHFW transmitters reside at C-site in the RF building. The frequency of these waves is 30 MHz, with multi-MW power levels possible.
HIS	Hardwired Interlock System	A legacy phrase for the relay-based system used to provide interlocking, ESTOP, access control, and enable/arm functionality on TFTR, NSTX, and the FY-15 & -16 operations of NSTX-U.
HMI	Human Machine Interface	A mechanism for operators to interact with the system. The HMI includes indicators and controls. The HMI may be a touchscreen.
	Logic Solver	A PSS-SIS device that performs logical control over PSS-SIS features

	Loop-set	A mode where the search and secure process for a securable area is complete
	Loop-drop	The condition that exists when the search & secure (Loop-set) is no longer valid.
	Lockable Area	Areas where access control is based on Trapped Keys and similar sequential locking mechanisms.
	LOCKDOWN	A state where secured area doors' ACAMs card readers are disabled if present and interlocked equipment is prohibited to run and is in a safe state. This state results from a PSS-SIS Emergency Stop.
	Movable Shielding	In the context of NSTX-U, movable shielding refers to various large concrete seal doors which form a part of the radiological boundary.
MER	Mechanical Equipment Room	The MER is located below the NTC, at the basement level. Numerous penetrations in the NTC floor provide access to the MER, filled with only cables, pipes, and firestops.
MPTS	Multi-Pulse Thomson Scattering	A diagnostic that uses a Class 4 Nd:YAG laser to pass 1060 nm laser light through the plasma; some light is scattered off the plasma particles and is collected and analyzed to measure the plasma temperature and density.
NB	Neutral Beams	These systems provide high power beams of neutral deuterium to heat the plasma. They result in the generation of 2.45 MeV neutrons by D-D fusion reactions. They have both low voltage systems (the arc and filament), and high voltage (to accelerate the beams).
CCR	NSTX-U Central Control Room	The CCR is located in the basement of the LSB. It is the facility for centralized operation of NSTX-U, including: operations, monitoring, coordination and initiation of normal (non-fault) mode changes, supplemental annunciation of conditions.
	NO ACCESS	A state where access to an exclusion area is prevented. Any interlocked systems within that space may be in an unsafe state. If the area is not in ACCESS state, it is in this state. All doors will be locked.
NTC	NSTX-U Test Cell	The room containing the NSTX-U machine, neutral beam units, and many diagnostics. The ECH generators and HHFW transmission lines and antenna components are also in the NTC.
PSS-SIS	Personnel Safety System - Safety Instrumented System	Safety Instrumented System used to provide access control, configuration verification and e-stop functionality for areas requiring hazard mitigation in addition to other protection layers..
	Permissive	A signal from the CCS that gives simple permission for a sub-system to operate.
	PSS-SIS Interlocked Device	Devices interlocked by the PSS-SIS. These devices are selected on the criteria of: ● presenting unacceptable risk in the unmitigated analysis and ● not having other mitigation strategies to fully mitigate the hazard in the absence of the PSS-SIS
OM	Other Methods	Means of mitigating hazards that do not require SIL rated reductions
	Safe	A condition that exists in an exclusion area when interlocked devices are not capable of creating hazards in that area. Note that the determination of an area being safe is not determined by the mode of the PSS-SIS, but rather by the status of the interlocked systems.
	Safeguard	A protection capability where personnel are protected from the threat by adding a barrier to prevent experimental hazard access,i.e., Thermal, Electrical, and Mechanical.
SIS	Safety Instrumented System	An engineered system whose design is guided by IEC 61511/61508 using active instrumented controls to mitigate hazards.
S&S	Search and Secure	The process that is utilized to establish that no personnel are remaining in an exclusion area.
SIF	Safety Instrumented Function	Safety Instrumented Functions are the most critical functions of the PSS-SIS required in order to prevent exposure of workers and the public to hazards.
SLD	Safety Lockout Device	The SLD provides a manual means of removing the air supply to the pneumatically operated FCPC Safety Disconnect Switches (SDS) and FCPC Grounding Switches once they are all in their safe position (FCPC Safety Disconnect Switches open and FCPC Grounding Switches closed).

	Securable Area	A lockable area that is monitored for door violations while unsafe.
	Shutdown/ Terminate	The action of rendering hazardous energy sources safe upon an emergency stop or access violation condition.
SIL	Safety Integrity Level	Safety integrity level (SIL) is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a safety instrumented function (SIF).
	Tamper Door	Door that covers a device that requires tamper resistance
	Unsafe	A condition that exists in an exclusion area when it is not demonstrably safe.

Table 2.0-2: *Assumptions*

Assumption Identification	Assumption
PSS-A01	Opening breakers interrupts power to downstream devices.
PSS-A02	Positioned and configured shielding is sufficient to block direct ionizing radiation.
PSS-A03	A direct ionizing radiation hazard will not occur in exclusion areas from the Neutral Beam (NB) system without both NB arc/filament and NB high voltage acceleration being present at the same time.
PSS-A04	A plasma supporting direct ionizing radiation cannot be sustained inside of the NSTX-U vacuum vessel without TF, OH, PF5 and PF3 coils simultaneously operating.
PSS-A05	HHFW cannot independently produce a direct ionizing radiation hazard.
PSS-A06	Standard Industrial Hazards will be primarily mitigated by systems independent from the PSS.
PSS-A07	PSS will not be required to provide mitigation for machine protection.
PSS-A08	Meeting the requirements of SRD-12, RD-24, RD-26, RD-27 results in the PSS-SIS meeting or exceeding a Safety Integrity Level of 1.
PSS-A09	PSS-SIS SIF redundancy is achieved with dual input devices, dual output devices, and a single-platform PLC with redundant processors capable of the minimum performance requirements as defined by SRD-12 and RD-24.
PSS-A10	The existing “dummy breaker” in the S1B1 cabinet will be replaced by an active component which will become ESF1-SB01.
PSS-A11	Breakers interdicted by the PSS-SIS will be modified to include undervoltage trip devices.

3.0 Personnel Safety System (PSS) Safety Instrumented System (SIS)

Note: Elaboration on these requirements are provided in the PSS-SIS RD (NSTX-U-RQMT-RD-024) [2].

3.1 Functions

The PSS-SIS functions and sub-functions are provided below.

3.1.1 PSS-SIS Functions

3.1.1.1 PSS-SIS Safety Instrumented Functions

a. PSS-SIS Safety Instrumented Functions and their required minimum risk reduction factors shall be defined by the Layer of Protection Analysis per Ref [9].

***Table 3.1.1.1-1**: PSS-SIS safety instrumented functions*

SIF	Description	Minimum Safety Integrity Level*
S-1.a	Interdict Interlocked Devices on Access Violation of the NTC North Shield Door[1]	SIL 1
S-1.b	Interdict Interlocked Devices on Access Violation of the NTC South Entryway Door	SIL 1
S-1.c	Interdict Interlocked Devices on Access Violation of the NTC West Shield Door	SIL 1
S-1.d	Interdict Interlocked Devices on Access Violation of the NTC South Shield Door	SIL 1
S-1.e	Interdict Interlocked Devices on Access Violation of the MER Mezzanine Entryway Door	SIL 1

*Based on Layer of Protection Analysis per Ref [9]

3.1.1.2 PSS-SIS Additional Actions

b. Prevent operation of interlocked devices when personnel have access to exclusion area.

c. Prevent personnel from accessing areas where interlocked devices may be capable of creating a hazard.

d. Provide E-STOP button functionality for interlocked devices.

e. Monitor personnel door status and interdict interlocked devices upon a door violation and/or emergency exit from the doors in Table 3.1.1.2-1

[1] This is the hinged "battleship door"

***Table 3.1.1.2-1**: Additional action areas*

1	Personnel doors on the cable spread room
2	Personnel doors on the TFTR test cell basement caged area

3.1.1.3 PSS-SIS Additional Functions

a. Provide engineered support for search and secure functions for exclusion areas.
b. Provide audible and visual warnings of unsafe status for each securable area.
    i. Provide audible and visual warnings within each securable area when transition from safe to unsafe status of the securable area is underway.
    ii. Provide a display near primary personnel entryways to securable areas showing the securable area status, the ACCESS system state, etc.
f. Provide centralized display of the NSTX-U Safety System (PSS) status and its associated equipment.

3.2 Materials and Design Requirements

3.2.1 Standards

a. The DOE Orders and Federal Regulations in Table 3.2.1-1 impose requirements for this design.

***Table 3.2.1-1**: DOE Requirements Sources*

1	DOE O 420.2 C [4]	*Safety of Accelerator Facilities*
2	DOE G 420.2-1A [5]	Accelerator Facility Safety Implementation Guide for DOE O 420.2C, Safety of Accelerator Facilities
3	10 CFR 835 [6]	Occupational Radiation Protection Program
4	10 CFR 851 [7]	Worker Safety and Health Program

b. PPPL Environment, Safety, and Health Directives ESHD 5008 [8] imposes requirements for this design.

c. The ANSI/IEC consensus standards in Table 3.2.1-2 provide guidance for this design.

***Table 3.2.1-2**: Consensus standards providing guidance for the design*

1	IEC 61511 [9]	Functional Safety - Safety instrumented systems for the process industry sector

3.2.2 Design Requirements

a. The Personnel Safety System (PSS-SIS) shall provide interlock and alarm devices, which when coupled with other safety layers, reduce the risk of an identified hazard risk/severity to "Acceptable" or "Desirable" as per the NSTX-U Project's accepted risk methodology [10].

b. The determination of the inclusion or exclusion of devices interlocked through the PSS-SIS shall be made during the hazard assessment for each facility or modification.

c. The fail-safe mode for each PSS-SIS signal input and output interface shall be defined.

d. The fail-safe mode of PSS-SIS controls shall be its de-energized state (i.e. zero volts for electrical signals, and/or loss of communication, that would render the controlled device to its safe state).

e. The features of the PSS-SIS which support Safety Functions shall be tamper resistant. Fielded components of the PSS-SIS shall have unique labels identifying the equipment as part of the PSS-SIS and allowing identification of components.

f. The features of the PSS-SIS which support Safety Functions shall be testable.

g. The PSS-SIS design, implementation, testing, and training shall be consistent with the use of the system as a credited control under the accelerator safety order (ASO) [5,6].

h. The PSS-SIS shall have the capability to detect inconsistent states of interlocked equipment relative to the desired state. This includes the state of the credited energy isolating devices, and may also include the state of non-credited isolation devices.

i. The PSS-SIS shall be an islanded system without connection to non PSS-SIS networks.

j. The PSS-SIS shall comply with laboratory Cyber Security requirements as applicable Ref [17].

k. The PSS-SIS software shall be documented in accordance with the laboratory Software Quality Assurance Plan as applicable Ref [18].

3.3: Configuration Requirements and Essential Features

a. The PSS-SIS shall not rely on the standard PPPL card reader system (ACAMS) for the implementation of Safety Functions.

b. If digital processing elements are utilized, methods shall be deployed to shutdown interlocked devices in the event of a significant timing or internal processing errors (e.g. watchdog timers).

c. The status of any interlocked equipment which is interlocked through the PSS-SIS shall be sensed by the PSS-SIS.

d. The PSS-SIS shall display Safe/Unsafe status and provide centralized control from the NSTX-U control room including but not exclusive to:
    a. Alarm/Fault reset
    b. PSS-SIS status
    c. Interlocked Equipment status

e. PSS-SIS equipment shall be rated for a defensible range of environmental parameters for the locations where they are installed; otherwise environmental parameters shall be monitored during PSS-SIS operation.

f. The PSS-SIS shall have means to annunciate status inside and outside of exclusion areas.

g. The PSS-SIS shall log critical data in a fashion which allows after-the-fact studies, but does not interfere with the execution of any safety function.

h. The PSS-SIS shall provide a means to support test requirements of PSS-SIS interlocked equipment.

i. The systems in Table 3.3-1 shall be interlocked by the PSS-SIS, reverting to a shutdown state in the event of a PSS-SIS Emergency Stop.

Table 3.3-1*. List of PSS-SIS Interlocked Systems*

	System	SBS # [1]
1	Variable Frequency Breakers	1.5.1.1.4
2	Selected Fixed Frequency Breakers	1.5.1.1.1

j. A latched PSS-SIS Emergency Stop shall be declared upon any one condition in Table 3.3-2 occuring.

***Table 3.3-2**. Conditions for declaring a PSS-SIS Emergency Stop*

	Condition
1	Activation of an E-STOP button
2	Opening of a monitored door to a secured area when PSS-SIS interlocked equipment is in an unsafe state
3	Inconsistent status between the allowed and present state of Interlocked equipment if interlocked equipment is in an unsafe state
4	Internal or timing error in digital processing elements (if applicable)
5	Actuation of the (TKS) Emergency Egress push-button when PSS-SIS interlocked equipment is in an unsafe state

k. Upon the occurrence of a PSS-SIS Emergency Stop, the steps in Table 3.3-3 shall be taken.

***Table 3.3-3**. Actions to take upon the declaration of a PSS-SIS Emergency Stop*

1	Transmission of shutdown signal to the CCS
2	Shutdown of all PSS-SIS interlocked systems after an allowed delay
3	Place all securable areas in a LOCKDOWN state

l. Areas whose access is monitored by the PSS-SIS shall include those in Table 3.3-4.

***Table 3.3-4**. Areas whose access is monitored by PSS-SIS*

1	NSTX-U Test Cell
2	Mechanical Equipment Room Mezzanine

3.4 Baseline Performance and Operational Requirements

a. PSS-SIS Interlocked Device shall be changed to safe state in a maximum of 4 seconds following the activation of a PSS-SIS Emergency Stop.

b. The time required to transition from NO ACCESS state to when hazards are applied shall be at least 300 seconds.

c. The PSS-SIS shall be capable of sending output signals to CCS as further defined in Ref [11]

3.5 Upgrade Performance and Operational Requirements

a. The PSS-SIS shall be designed to support expansion of NSTX-U facility capabilities, in terms of both systems that are interlocked and number of exclusion areas

3.6 Interfaces

***Table 3.6-1**: Interfaces for the NSTX-U Personnel Safety System, Logic Solver & Logic, I/O, I/O Devices, Interdiction Devices (SBS 1.7.3.1.1)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.8	Central Control System (CCS)	Electrical Signal	PSS digital output module to CCS digital input module.	The PSS-SIS provides limited status and permissive information to the CCS.	CWD
1.5.1.1.4	SV Switchgear	Electrical Signal	Undervoltage trip circuit and permit to close on breaker	13.8 SV1 & SV2 breakers to FCPC thyristor rectifiers (SV1-SB01 through SV1-SB09, SV2-SB01 to SV2-SB09, SV1-SB12, SB2-SV12) are opened upon a PSS-SIS Emergency Stop	Electrical Schematic
1.5.1.1.4	SV Switchgear	Diagnostic	Where sensor mounts to cabinet/conductor	Position indicators on SV1 and SV2 breakers used to assess the status of breakers by PSS-SIS.	Electrical Schematic
1.5.1.1.4	SV Switchgear	Electrical Signal	Undervoltage trip circuit and permit to close on breaker	Variable frequency 13.8 kV breakers to NB power supplies (ESV2-SB10, ESV2-SB11) are opened upon a PSS-SIS Emergency Stop	Electrical Schematic
1.5.1.1.4	SV Switchgear	Diagnostic	Where sensor mounts to cabinet/conductor	Position indicators on 13.8 kV breakers to NB power supplies (ESV2-SB10, ESV2-SB11) used to assess the status of breaker by PSS-SIS.	Electrical Schematic
1.5.1.1.1	AC Breakers and Switchgear	Electrical Signal	Undervoltage trip circuit and permit to close on breaker	Fixed frequency 13.8 kV breaker to S1-B1 feeding MG exciter opened upon a PSS Emergency Stop	Electrical Schematic
1.5.1.1.1	AC Breakers and Switchgear	Diagnostic	Where sensor mounts to cabinet/conductor	Position indicators on S1-B1 breaker used to assess the status of breaker by PSS-SIS.	Electrical Schematic
1.5.1.1.1	AC Breakers and Switchgear	Electrical Signal	Undervoltage trip circuit and permit to close on breaker	Fixed frequency 13.8 kV breaker to NB high voltage power supplies (ESF1-SB10) are opened upon a PSS Emergency Stop	Electrical Schematic
1.5.1.1.1	AC Breakers and Switchgear	Diagnostic	Where sensor mounts to cabinet/conductor	Position indicators on fixed frequency 13.8 kV breaker (ESF1-SB10) for NB high voltage power used to assess the status of breaker by PSS.	Electrical Schematic
1.5.1.1.1	AC Breakers and Switchgear	Electrical Signal	Undervoltage trip circuit and permit to close on breaker	Fixed Frequency 13.8 kV breaker (ESF2-SB05) for NBI 480 VAC pulsed power (arc and filament supplies) are opened upon a PSS-SIS Emergency Stop	Electrical Schematic
1.5.1.1.1	AC Breakers and Switchgear	Diagnostic	Where sensor mounts to cabinet/conductor	Position indicators on fixed frequency 13.8 kV breaker (ESF2-SB05) for NBI 480 VAC pulsed power used to assess the status of breaker by PSS-SIS.	Electrical Schematic
1.5.3.1.2	TF Disconnect Switches	Diagnostic	Where sensor mounts to the disconnect switch	PSS-SIS detects the position of the TF disconnect switches	Mechanical Drawing

1.5.3.1.3	TF Ground Switches	Diagnostic	Where sensor mounts to the ground switch	PSS-SIS detects the position of the TF ground switches	Mechanical Drawing
1.5.3.2.3	OH Ground Switch	Diagnostic	Where sensor mounts to the ground switch	PSS-SIS detects the position of the OH ground switches	Mechanical Drawing
1.5.3.2.2	OH Disconnect Switch	Diagnostic	Where sensor mounts to the disconnect switch	PSS-SIS detects the position of the OH disconnect switches	Mechanical Drawing
1.5.3.3.3	PF Ground Switches	Diagnostic	Where sensor mounts to the ground switch	PSS-SIS detects the position of the PF ground switches	Mechanical Drawing
1.5.3.3.2	PF Disconnect Switches	Diagnostic	Where sensor mounts to the disconnect switch	PSS-SIS detects the position of the PF disconnect switches	Mechanical Drawing
1.2.4.6	Neutral Beam Power System	Diagnostic	Where sensor mounts to Ross Grounding Switch	PSS-SIS detects the position of the NBI Ross ground switches	Mechanical Drawing
1.2.4.6	Neutral Beam Power System	Diagnostic	Where sensor mounts to Pringle switch	PSS-SIS detects the position of the NBI Pringle switches	Mechanical Drawing
1.5.3.1.8	TF PCTS components	Diagnostic	Where sensor monitors TF bus links	PSS-SIS detects the position of the TF bus links in PCTS	Mechanical Drawing
1.5.3.2.8	OH PCTS components	Diagnostic	Where sensor monitors OH bus links	PSS-SIS detects the position of the OH bus links in PCTS	Mechanical Drawing
1.5.3.3.8	PF PCTS components	Diagnostic	Where sensor monitors PF bus links	PSS-SIS detects the position of the PF bus links in PCTS	Mechanical Drawing
1.5.3.5	PCTS Frame and Structures	Structural	Where sensor mounts to PCTS	PSS-SIS detects the position of the bus links in PCTS	Mechanical Drawing
1.5.1.2	D-Site Auxiliary Power	Electrical Power	various	Electrical power for the PSS-SIS from D-Site Auxiliary Power	Electrical Schematic for Directly Wired Components
0.1.1.11	C-Site Power	Electrical Power	various	Electrical power for the PSS-SIS from C-Site Power	Electrical Schematic for Directly Wired Components
1.8.1.1.4	NTC Walls	Structural	At NTC wall	Components of the PSS-SIS are supported by the test cell wall	N/A
1.8.1.1.1	NTC Platforms	Structural	At platform	Components of the PSS-SIS are supported by the test cell platforms	N/A
1.7.3.10.2	Trapped Key Status Monitoring	Electrical Signal	At PSS-SIS input block	PSS-SIS monitors the status of select key blocks of the TKS	CWD
0.1.1.6	Other D-Site Physical Infrastructure	Diagnostic	At cage doors	PSS-SIS monitors doors on the Cable Spread Room	CWD
0.1.1.6	Other D-Site Physical Infrastructure	Diagnostic	At cage doors	PSS-SIS monitors doors to the TTC cable cage	CWD
1.8.1.1	Test Cell	Diagnostic	At doors	PSS-SIS monitors personnel doors to the NSTX Test Cell	CWD
1.8.1.1	Test Cell	Diagnostic	At doors	PSS-SIS monitors positions of shield doors to the NSTX Test Cell	CWD
1.7.3.1.2	PSS Network	Fiber Optic	At fiberoptic connectors	PSS network interfaces the various PSS logic solver and IO devices	Schematic

***Table 3.6-2**: Interfaces for the NSTX-U PSS-SIS Network (SBS 1.7.3.1.2)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.1.1	PSS Logic Solver & Logic, I/O, I/O Devices, Interdiction Devices	Fiber Optic	At fiber optic connectors	PSS network interfaces the various PSS logic solver and IO devices	Schematic
1.7.3.1.3	PSS Conduit, Wire, Fiber	Structural	---	Network fiber optics are run in conduits	Schematic
1.7.3.1.8	HMI	Electrical Signal	At network connection	PSS network provides information to the HMI	Schematic

Table 3.6-2: *Interfaces for the NSTX-U Personnel Safety System, conduit, wire, and fibers (SBS 1.7.3.1.3)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.8.1.1.1	NTC Platforms	Structural	Where conduit is clamped to platform or columns	Conduits for PSS-SIS Supported by NTC platforms and platform columns	Conduit Drawing
1.8.1.1.4	NTC Walls	Structural	Where conduit is clamped to wall	Conduits for PSS-SIS Supported by NTC walls	Conduit Drawing
1.8.1.1.5	NTC Penetrations	Wall/Floor Penetration	At surface of conduits	Conduits for PSS-SIS pass through NTC Penetrations	Conduit Drawing
0.1.1.6	Other D-Site Physical Infrastructure	Wall/Floor Penetration	Various	Conduits for PSS-SIS are distributed in various locations through D-Site	Conduit Drawing
0.1.1.6	Other D-Site Physical Infrastructure	Structural	Various	Conduits for PSS-SIS pass through various D-Site wall penetrations	Conduit Drawing
1.5.3.3.1	PF SDS	Structural	Where conduit joins to the cabinet	Conduits for PSS-SIS interface with the PF SDS cabinets	Conduit Drawing
1.5.3.2.1	OH SDS	Structural	Where conduit joins to the cabinet	Conduits for PSS-SIS interface with the TF SDS cabinets	Conduit Drawing
1.5.3.1.1	TF SDS	Structural	Where conduit joins to the cabinet	Conduits for PSS-SIS interface with the OH SDS cabinets	Conduit Drawing
1.5.1.1.1	AC Breakers and Switchgear	Structural	Where conduit joins to the cabinet	Conduits for PSS-SIS interface with some fixed frequency 13.8 kV breaker cabinets	Conduit Drawing
1.5.1.1.4	SV Switchgear	Structural	Where conduit joins to the cabinet	Conduits for PSS-SIS interface with the variable frequency 13.8 kV breaker cabinets	Conduit Drawing
1.8.1.1.1	NTC Platforms	Structural	At platform	Conduits of the PSS-SIS are supported by the test cell platforms	Conduit Drawing
1.8.1.1.4	NTC Walls	Structural	At NTC wall	Conduits of the PSS-SIS are supported by the test cell wall	Conduit Drawing
1.2.4.6	Neutral Beam Power System	Structural	Where conduit mounts to walls	Conduit for PSS-SIS is mounted to, and interfaces with, neutral beam power equipment.	Conduit Drawing
1.7.3.1.2	PSS Network	Structural	---	Network fiber optics are run in conduits	Conduit Drawing
1.7.3.1.4	PSS Enclosures & Misc. Hardware	Structural	At enclosure walls	PSS conduits interface to PSS enclosures	Conduit Drawing

***Table 3.6-1**: Interfaces for the PSS-SIS Enclosures and Misc. Hardware (SBS 1.7.3.1.4)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.1.3	PSS Conduit, Wire, Fiber	Structural	At enclosure walls	PSS conduits interface to PSS enclosures	Schematic
1.7.3.10.1	Trapped Key Hardware & Sequencing	Structural	Where switch is mounted	Trapped key plocks mounted on PSS S&S station enclosures	Mechanical Drawing
1.7.3.1.5	PSS Security Fasteners	Structural	At fastener	Security fasteners are used to ensure that contents of enclosures are not tampered with	Schematic

***Table 3.6-1**: Interfaces for the PSS-SIS Security Fasteners (SBS 1.7.3.1.5)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.1.4	PSS Enclosures & Misc. Hardware	Structural	At fastener	Security fasteners are used to ensure that contents of enclosures are not tampered with	Schematic

***Table 3.6-1**: Interfaces for the PSS-SIS HMI (SBS 1.7.3.1.8)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.1.2	PSS Network	Electrical Signal	At network connection	PSS network provides information to the HMI	Schematic
0.1.1.11	C-Site Power	Electrical Power	At plug	C-site elements of the HMI require power	---

4.0 Trapped Key System

Note: Specific systems and sequences are defined in (NSTX-U-RQMT-RD-026) [12].

4.1 Functions

The functions of the Trapped Key System (TKS) include:

a. Provide a means to positively assure that specified areas are in a secured configuration before hazards are introduced to that area.

b. Provide a means to positively assure that specified safeguards are in proper configuration before the protected component is placed in a hazardous condition.

c. Provide status of key positions to the Chief Operating Engineer per Ref [12].

4.2 Materials and Design Requirements

4.2.1 Standards

a. PPPL Environment, Safety, and Health Directives ESHD 5008, Section 2 Chapter 5 [8] imposes requirements for this design.

4.2.2 Design Requirements

a. The trapped key system shall implement a specific engineered sequence of actions to ensure that access points are closed and safeguards are in place before protected components are put in an unsafe state.

b. The trapped key systems shall be capable of handling multi-layer sequences.

c. Specific safeguards such as moveable guards may utilize the Trapped Key System.

d. The trapped key system shall not be able to be bypassed with common tools.

e. The keys of the TKS shall be clearly labeled for their interface.

f. The keys shall have a feature to deter carrying the keys away from experimental areas (i.e. 'pocketing').

4.3 Configuration Requirements and Essential Features

a. The trapped key system shall provide status of key summation blocks to the CCS and/or PSS-SIS. Specific details of this status information are provided in Ref. [12].

b. The trapped keys shall be Safety Integrity-level capable as determined necessary by safety analysis.

c. Trapped Keyed doors/gates enclosing occupiable volumes shall have a means to unlock the door/gate from inside the enclosed area, or shall have kick-out panels or equivalent to enable egress by any individual trapped in those areas.

4.4 Baseline Performance and Operational Requirements

N/A

4.5 Upgrade Performance and Operational Requirements

a. The TKS shall be designed to support expansion of NSTX-U facility capabilities, in terms of both systems that are interlocked and number of exclusion areas.

4.6 Interfaces

Table 4.6-1: *Interfaces for the NSTX-U Trapped Key Hardware and Sequencing (SBS 1.7.3.10.1)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.9.1	Caged Areas	Structural	Where TF trapped key hardware mounts to the cage and cage door.	TKS ensures that doors to cages are closed during operations. These include the gallery cages, bakeout cage, TTC ground cage, cable spread room, TTC buswork caged area, and three vestibules (north door, south door, MER mezzanine).	Mechanical Drawing
1.2.1.7	HHFW Transmission Lines	Structural	On Coaxial switches above the RFE	TKS ensures that the RF baseball switches are in a position to prevent power from entering the NTC when access is allowed	Mechanical Drawing
1.2.4.7	Neutral Beam Control Systems	Electrical Signal	At LCC	TKS inhibits the enabling of primary power when access to the test cell and related areas is allowed.	Schematic(s))
1.5.4	FCPC Control and Protection Systems	Structural	At the SLD	Trapped key block mounted to SLD	Mechanical Drawing
1.7.3.10.2	Trapped Key Status Monitoring	Electrical Signal	COTS interface	The various key blocks are monitored by the TKS monitoring system.	Schematic(s))
1.7.3.9.2	Bus Work Guards & Exposed Conductors >50V Guards	Structural	Various depending on the physical interface	The TKS is utilized to ensure proper configuration of moveable safeguards for exposed electrical conductors.	Mechanical Drawing
1.8.1.1.4	NTC Walls	Structural	TBD	TKS uses components mounted to NTC walls	Mechanical Drawing
1.7.3.1.4	PSS Enclosures & Misc. Hardware	Structural	Where switch is mounted	Trapped key plocks mounted on PSS S&S station enclosures	Mechanical Drawing
1.3.3.4	Bakeout PLC and Controls	Structural		Trapped key block mounted to control cabinet	Mechanical Drawing
0.1.1.6	---	Structural		Trapped key blocks mounted in various locations throughout D-Site	Mechanical Drawing
1.5.1.1.1	AC Breakers and Switchgear	Structural	At surface of SF2-B05 breaker cubicle	TKS block mounted to beaker cubicle	Mechanical Drawing

***Table 4.6-2**: Interfaces for the NSTX-U Trapped Key Monitoring (SBS 1.7.3.10.2)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.10.1	Trapped Key Hardware & Sequencing	Electrical Signal	COTS interface	The various key blocks are monitored by the TKS monitoring system.	Schematic
1.8.1.1.4	NTC Walls	Electrical Signal	Movable shield wall control enclosure	TKS disables movable shield wall controls	Schematic
1.7.3.1.1	PSS Logic Solver & Logic, I/O, I/O Devices, Interdiction Devices	Electrical Signal	At PSS-SIS input block	PSS-SIS monitors the status of select key blocks of the TKS	CWD
1.7.3.8	Central Control System (CCS)	Electrical Signal	Isolation transformers	Status of select key blocks provided to CCS	Mechanical Drawing
1.3.3.4	Bakeout PLC and Controls	Electrical Signal	At PLC input block	Bakeout PLC monitors the status of select TKS keys	CWD
1.5.4.6	Safety Lockout Device (SLD)	Electrical Signal	At SLD enclosure	The TKS prevents the SLD from pressurizing when access is allowed in the NTC.	CWD
1.5.1.1.1	AC Breakers and Switchgear	Electrical Signal	Wiring interface within SF2-B05 breaker cubicle	TKS prevents the breaker from closing via removal of permit to close	Schematic

5.0 Configuration Managed Safeguards

Note: Elaboration on these requirements are provided in the Configuration Managed Safeguards RD (NSTX-U-RQMT-RD-027) [13].

5.1 Functions

a. Provide physical safeguards to protect personnel from specific contact industrial hazards as identified in the hazard analysis of the HAR [15] and SAD [14].

b. These hazard types are broken into 5 categories in the NSTX-U SBS as per Table 5-1.

***Table 5-1**: Safeguard Categories by SBS*

1.7.3.9.1	Caged Areas	This category involves placing cages in areas that prevent individuals from coming in contact with potential equipment hazards.

1.7.3.9.2	Bus Work Guards & Exposed Conductors >50V Guards	This category involves covers over exposed conductors whose voltage exceeds 50 V, as per the PPPL Safety Manual Section 2.
1.7.3.9.3	Helium Piping Guards	This category involves covers over the piping insulation for the NSTX-U helium system. This system conveys pressurized helium at up to 450 ℃ from the D-site pump room to the NSTX-U device using insulated supply and return pipes. The exterior surface of the insulation is touch-safe and the safeguards function to prevent contact with the elevated temperature piping contained within the insulation.
1.7.3.9.4	Laser Flight Tube Guards	This category includes guards within the NSTX-U test cell that function to prevent exposure of individuals to laser light.
1.7.3.9.5	NSTX-U Vacuum Window >4" Guards	This category includes vacuum window guards for windows greater than 4" in diameter, as required by the Safety Manual, Section 9 chapter 14. These function to prevent i) breakage of the window resulting in an individual being drawn toward the vacuum, and ii) propulsion of window fragments towards individuals in the event of a vessel overpressurization.
1.7.3.9.6	NSTX-U RF Wave Guide Guards	This category includes guards that prevent contact exposure to electrical hazards >50 volts from an RF source.

Note: More generic safeguards on D-Site pumps, HVAC equipment, machine tools, etc. are not considered here. The scope under consideration here involves only hazards within NSTX-U experimental areas, which are associated with the operation of NSTX-U experimental systems.

5.2 Materials and Design Requirements

a. PPPL Environment, Safety, and Health Directives ESHD 5008 Section 2 Chapter 4 [8] imposes complimentary requirements for this design.

b. Specific safeguarded areas and systems shall be listed in RD-027 Configuration Controlled Safeguard Requirements.

5.3: Configuration Requirements and Essential Features

a. The safeguards shall not interfere with the function of the components.

b. The safeguard design shall provide a means to access equipment when the safeguard is removed.

c. The safeguards shall be placed under configuration management as defined in Table 5.3-1.

d. Safeguards as defined here shall be clearly labelled as such in their deployed condition.

e. The configured controlled safeguards shall prevent personnel from accessing the corresponding hazard(s) unless they have tools or keys to remove the safeguard.

f. The configuration managed safeguards shall be secured and be tamper resistant.

g. The configuration managed safeguards shall not create a new hazard.

Note: in some cases (e.g. optics), the safeguard may have other primary functions

Table 5.3-1*: Interpretation of configuration management for the purpose of this SBS.*

#	Configuration Management Option
1	The safeguards may be locked in place by the trapped key system, preventing energization of the underlying hazard unless the guards are present. See *NSTX-U-RQMT-RD-027*
2	The presence of safeguards may be tracked by administrative procedures.

5.4 Baseline Performance and Operational Requirements

N/A

5.5 Upgrade Performance and Operational Requirements

a. The Configuration Managed Safeguards shall be designed to support expansion of NSTX-U safeguarded locations.

5.6 Interfaces

Table 5.6-1*: Interfaces for the Configuration Managed Safeguards - Caged Areas (SBS 1.7.3.9.1)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.10.1	Trapped Key Hardware & Sequencing	Structural	Where TF trapped key hardware mounts to the cage and cage door.	TKS ensures that doors to cages are closed during operations. These include the gallery cages, bakeout cage, TTC ground cage, cable spread room, TTC buswork caged area, and three vestibules (north door, south door, MER mezzanine).	Mechanical drawings
1.8.1.1.1	NTC Platforms	Structural	At the brackets mounting the cage components to the platforms and columns	NSTX-U Machine Perimeter Safeguards may mount to NTC platforms and their supports	Mechanical drawings
1.8.1.1.8	NTC Floor	Structural	At the brackets mounting the cage components to the floor	NSTX-U Machine Perimeter Safeguards may mount to NTC floor	Mechanical drawings
0.1.1.6	Other D-Site Physical Infrastructure	Structural	At brackets that mount cages to floors/walls	Various cages mount to floors and walls in the gallery, pump room, and elsewhere.	Mechanical drawings

***Table 5.6-2**: Interfaces for the Configuration Managed Safeguards - Bus Work Guards & Exposed Conductors >50V Guards (SBS 1.7.3.9.2)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.10.1	Trapped Key Hardware & Sequencing	Structural	Various depending on the physical interface	The TKS is utilized to ensure proper configuration of moveable safeguards for exposed electrical conductors.	Mechanical Drawing(s)
1.1.3.4	Bus Bar Systems and Bus Tower	Spatial	Where safeguard mounts	Safeguards are used to deter individuals from touching otherwise exposed coil bus work in the NSTX-U test cell.	Mechanical Drawing(s)
1.3.5.1.1	GDC + Filament Power Supplies	Spatial	Where safeguard mounts	Safeguards are used to deter individuals from touching conductors which may be at vacuum vessel potential (i.e. elevated during high pots of the vacuum vessel)	Mechanical Drawing(s)
1.3.5.1.2	In-Vessel GDC Probes + Filaments	Spatial	Feedthrough	Safeguards are used to deter individuals from touching otherwise exposed high voltage terminals on the GDC system in the NSTX-U test cell.	Mechanical Drawing(s)
1.3.4.3.2	Massive gas injectors	Spatial	Control Racks	Safeguards are used to deter individuals from touching otherwise exposed high voltage terminals on the MGI system in the NSTX-U test cell.	Mechanical Drawing(s)
1.4.1.8	MSE	Spatial	Where safeguard mounts	Safeguard are used to deter exposure to the high voltage of the MSE-LIF neutral beam components	Mechanical Drawing(s)
1.5.3.5	PCTS Frame and Structures	Structural	where barriers bolts to PCTS	Barrier ensures that bus links are not present.	Mechanical Drawing

***Table 5.6-3**: Interfaces for the Configuration Managed Safeguards - Helium Piping Guards (SBS 1.7.3.9.3)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.3.3.1.1	Helium Skid & Piping	Spatial	At surface of insulation	Safeguards are used to prevent individuals from coming in contact with the He piping used to supply hot He to the machine.	Mechanical drawings
1.3.3.1.2	Ex-Vessel Helium Manifolds	Spatial	At surface of insulation	Safeguards are used to prevent individuals from coming in contact with the He manifolds on the machine.	Mechanical drawings

6.0: Centralized Control System (CCS)

Note: Elaborations on these requirements are identified in the CCS RD (NSTX-U-RQMT-RD-025-00) [11].

6.1 Function

a. The function of the Centralized Control System is to provide centralized control of NSTX-U controlled equipment by the control room operations staff, by:
   i. Providing enable and arm permissives to controlled equipment capable of utilizing this information
   ii. Providing simple permissive signals to controlled equipment that do not have the capability to receive the full enable/arm permissive set.
   iii. Providing disable and disarm functionality for controlled equipment.
   iv. Provide an HMI to display the status and provide secure controls for operators and users.
b. Systems are selected for inclusion in the CCS by virtue of:
   i. having sufficient energy such that mis-operation could cause significant equipment damage.
   ii. requiring “Other Methods” hazard control in the safety analysis.
   iii. being critical to central control for proper conduct of operations.

Note: The CCS replaces the process control aspects of the TFTR-era HIS system. It is a subset of the full process control systems for NSTX-U, which include various PLCs, labview systems, and hardwired control systems. See interface table.

6.2 Materials and Design Requirements

a. The CCS should be designed to support expansion of NSTX-U facility capabilities.
b. The features of the CCS which support process control of controlled systems shall be testable.

6.3: Configuration Requirements and Essential Features

6.3.1: Systems Interfaced to the CCS

a. The CCS shall provide a permissive signal to local Basic Control Systems (BCS) to transition controlled equipment to and from the energized (hazardous) state.
b. The permissive signal may be the full set of enable/arm permissives, or simple permissives.
c. The NSTX-U CCS shall control the enabling and arming of the systems defined in Ref [11].
d. The NSTX-U CCS shall provide “No-NSTXU-ESTOP” signal to the local BCS for the systems in Ref [11]

6.3.2: PSS-SIS Interface Requirements

a. Interfaces between the CCS and the PSS-SIS shall not compromise the PSS-SIS safety function including possible failure modes on the CCS side of the interface.

b. In the event a PSS-SIS Emergency Stop is conveyed from the PSS-SIS, the CCS shall remove permissives, including removing No-NSTXU ESTOP, enable, and arm signals, to the numerous (local) BCS's. Details describing the specific response of each local BCS will be described in Ref [11].

6.3.3: HMI and Data Logging Requirements

a. A central control station for the CCS shall be provided at the CoE Station in the NSTX-U Control Room
b. The CCS shall have means to annunciate status of permissives for controlled systems, i.e., armed, enabled.
c. The CCS shall have means to control the status of permissives for controlled systems, i.e., armed, enabled.

6.4 Baseline Performance and Operational Requirements

Refer to Ref [11]

6.5 Upgrade Performance and Operational Requirements

a. The CCS shall log critical data in a fashion which allows after-the-fact studies but does not interfere with the execution of any function.
b. The CCS should receive status information from controlled devices.

6.6 Interfaces

Table 6.6-1: *Interfaces for the Centralized Control System (SBS 1.7.3.8)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.5.4.1	Hardwired Control System & PLC	Electrical Signal	FCPC Control Boards	The CCS provides permits to enable and arm the FCPC rectifiers (including the DC link rectifiers), and receives rectifier status signals	CWD, Electrical Schematics
1.5.2.4.1	SPA DC Link	Electrical Signal	FCPC Control Boards	The CCS provides enable and arm permissives for the DC link rectifiers.	CWD
1.4.1.3	Multi-pulse Thompson Scattering (MPTS)	Electrical Signal	At isolation transformers	CCS provides permissives (previously no E-STOP and Loop Set) to the MPTS Laser Interlock Box. This box uses these signals along with other MPTS related signals to determine the Laser Permissive and allow the laser guillotine to open	CWD
1.3.1.4	Vacuum System PLC	Electrical Signal	At I/O block of PLC	CCS provides equivalent to previously existing "No-Facility ESTOP" and "LOOP SET" equivalent signals to the vacuum system PLC	CWD

1.7.3.1.1	PSS Logic Solver & Logic, I/O, I/O Devices, Interdiction Devices	Electrical Signal	PSS digital output module to CCS digital input module.	The PSS-SIS provides limited status and permissive information to the CCS.	CWD
1.3.3.4	Bakeout PLC and Controls	Electrical Signal	interface between PLCs	The CCS provides No-ESTOP signal to the bakeout system.	CWD
1.2.3	Electron Cyclotron Pre-Ionization (ECH)	Electrical Signal	TBD	The CCS provides permits to enable and arm the ECH pre-ionization system, and receives status information from the system	CWD
0.1.1.11	C-Site Power	Electrical Power	At wall plug or panel	AC power is provided to the CCS installation at C-site	
1.4.1.8	MSE	Electrical Signal	Interface between PLCs	The CCS sends a No E-Stop Signal to the BCS controlling the MSE-LIF	CWD
1.3.2.4	Water System PLC	Electrical Signal	At isolation transformers	The CCS sends a No E-Stop signal to the PLC controlling the water systems (high pressure pump, low pressure pump, and OH Water Heater)	CWD
1.7.3.10.2	Trapped Key Status Monitoring	Electrical Signal	Isolation transformers	Status of select key blocks provided to CCS	CWD
1.2.4.7	Neutral Beam Control Systems	Electrical Signal	At isolation transformers	The CCS provides permits to enable and arm to the neutral beam systems, and receives status information on the enable/arm status from the neutral beams	CWD, Electrical Schematics
1.2.1	High Harmonic Fast Wave (HHFW)	Electrical Signal	At isolation transformers	The CCS provides permits to enable and arm to the HHFW systems, and receives status information on the enable/arm status from HHFW control system	CWD, Electrical Schematics
1.5.4.6	Safety Lockout Device (SLD)	Electrical Signal	At isolation transformers	The CCS provides permits to vent or pressurize the SLD and receives status information on the position of the SLD	CWD

7: Vessel and Diagnostic Ground Systems (SBS 1.7.3.2)

7.1 Functions

a. The vessel and diagnostic grounds provide single point grounds for these systems.

b. The NTC ground fault monitor (GFM) is utilized to assess loop faults for the NSTX-U vessel and diagnostic ground[2,3]

7.2 Materials and Design Requirements

There are no material or design requirements beyond those for standard electronics design for NSTX-U.

7.3: Configuration Requirements and Essential Features

7.3.1: Grounding of Experimental Equipment in the Test Cell

a. A dedicated connection of the vessel to earth ground shall be provided with low-inductance bus-bar.

b. There shall be a mechanism to open this ground for purpose of vessel isolation testing.

c. For specific racks containing equipment that is electrically referenced to the vessel, there shall be dedicated low-inductance bus-work referencing those racks to the vessel.

d. For diagnostic racks not requiring a vessel reference, a dedicated single point connection of diagnostic racks to ground shall be provided.

7.3.2: Grounding of Experimental Equipment in the Test Cell

a. The GFM shall be capable of identifying loop faults between the vessel ground, diagnostic ground, and building steel ground.

> *Note: Loop fault here refers to a connection between ground classes. The system need not detect ground faults, i.e. cases where the quality of the system's intended ground is compromised.*

b. This requirement removed in Rev. 2 of this document.

c. The system shall archive data with sufficient fidelity to determine when evolutions in the system loop impedance occured.

d. This archiving shall be include at least 1 week of data, with ability to download data for off-line examination.

e. It shall be possible to "blank" the ground fault detection during machine pulses.

f. The system shall accommodate high-pots and megger tests of the NSTX-U vessel.

g. This requirement removed in Rev. 2 of this document.

---

[2] NSTX and the FY-16 operation of NSTX-U had electrically isolated inner and outer vacuum vessels. The GFM thus monitored the ground status of both vessels. The lower ceramic insulator was removed during the Recovery Project, and therefore only a single vessel ground need be monitored.

[3] The test cell ground fault monitor should not be confused with the FCPC coil/rectifier ground fault monitors.

h. The system shall provide a visible or audible indication of a detected ground fault.

7.4 Baseline Performance and Operational Requirements

a. The GFM shall be capable of detecting loop faults with impedances from 0 Ohms up to at least 500 Ohms.

7.5 Upgrade Performance and Operational Requirements

a. There are no performance upgrades envisioned for the ground fault monitor

7.6 Interfaces

Table 7.6-1: *Interfaces for the Ground Fault Monitor Coils (SBS 1.7.3.2.1)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.2.2	Ground Fault Monitor PLC & Electronics	Electrical Signal	at electrical connection on chassis	Electronics use information sent to and received from these coils to assess the presence of loop fauls	Electrical Schematic
1.7.3.2.4	Diagnostic Ground Bus	Spatial	Where coils are mounted to the bar	Sense and transmit coils are mounted to the bars	Electrical Schematic
1.7.3.2.3	Vessel Ground Bus & Switch	Spatial	Where coils are mounted to the bar	Sense and transmit coils are mounted to the bars	Electrical Schematic

Table 7.6-2: *Interfaces for the Ground Fault Monitor PLC & Electronics (SBS 1.7.3.2.2)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.3.1.4	Vacuum System PLC	Fiber Optic	Serial link	Information is passed between these two PLCs	
1.5.1.2	D-Site Auxiliary Power	Electrical Power	At panel or plug	AC power is provided to the ground fault detector	
1.7.3.2.1	Ground Fault Monitor Coils	Electrical Signal	at electrical connection on chassis	Electronics use information sent to and received from these coils to assess the presence of loop fauls	Electrical Schematic

Table 7.6-3: *Interfaces for the Vessel Ground Bus & Switch (SBS 1.7.3.2.3)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.3.3.2.1	Bakeout Bus Work	Electrical Power	At connection of bakeout bus to ground connection	The ground connection to the vessel is made by connecting to the lower bakeout bus bars.	Electrical Schematic
1.7.3.2.1	Ground Fault	Spatial	Where coils are mounted	Sense and transmit coils are	Electrical Schematic

	Monitor Coils		the the bar	mounted to the bars	
1.8.1.1.7	NTC Racks	Electrical Power	Where bus is connected to the rack	Specific NTC rasks receive an electrical reference to the vessel ground	Electrical Schematic

***Table 7.6-4**: Interfaces for the Diagnostic Ground Bus (SBS 1.7.3.2.4)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.7.3.2.1	Ground Fault Monitor Coils	Spatial	Where coils are mounted the the bar	Sense and transmit coils are mounted to the bars	Electrical Schematic
1.8.1.1.7	NTC Racks	Electrical Power	Where bus is connected to the rack	Specific NTC rasks receive an electrical reference to diagnostic ground	Electrical Schematic

8: Radiation Monitoring System

8.1 Functions

a. The function of the NTC radiation monitor system (Neutron and Gamma Area Monitors) is to measure the neutron and gamma dose rates within the NTC to provide the appropriate alarm threshold for regulatory posting annunciation at the north and south entrance doors.

b. The function of the PPPL site boundary gamma and neutron integrating dose monitors is to provide data to be used to compute the annual site boundary dose rate for PPPL.

8.2 Materials and Design Requirements

N/A

8.3: Configuration Requirements and Essential Features

Test Cell Dose Rate Instruments

a. NTC dose rate instruments shall be mounted on each of four walls of the test cell, at approximately the 115’ elevation.

b. NTC dose rate instruments shall reside on a dedicated 120 volt circuit.

c. NTC dose rate instruments shall have hardwired internet connections with dedicated switches.

d. The NTC dose rate instruments shall be capable of operating remote relay contacts through internal electronics.

e. Relay for NTC dose rates shall be connected to visual annunciators located at the north and southeast test cell entrances.

f. The visual annunciators must be electrically isolated from the electronics inside the test cell as per the GRD [1].

g. When preset alarm conditions are met on any single monitor, it will trigger a condition resulting in the illumination of the external annunciators, indicating a high radiation field existing inside the NTC.

h. When the alarm condition clears the lighted annunciators indicating high radiation fields inside the NTC shall turn off, returning the test cell to its normal posting condition.

Boundary Trailers

i. There shall be stand alone integrating dose Gamma and Neutron monitors located in the north and east boundary trailers.

j. Boundary integrating dose rate monitors to include a backup for each trailer for redundancy.

k. Boundary integrating dose monitors shall be manually monitored.
   i. Prior to morning startup to collect background readings from the night before.
   ii. Following daily operations to collect the daily dose from operations.

8.4 Baseline Performance and Operational Requirements

a. Boundary trailer to have temperature/humidity control to maintain < 55% RH with temperature range of 40 - 75 degrees fahrenheit.

b. NTC test cell monitors shall be calibrated annually by the factory. Calibrated instruments shall be available for quick replacement.

c. The NTC area monitors shall be capable of measuring from 1 mR/hr to 1.0 R/hr over three decades.

d. The boundary trailer monitors shall be capable of measuring integrated dose with a lower limit of detectability of 1 microrem, with a maximum dose of 100 mrem full scale.

e. The boundary trailer monitors shall have a “overflow counter” to handle total counts in excess of 100 mrem (based on counts/mrem calibration).

8.5 Upgrade Performance and Operational Requirements

a. Visual annunciators may be required at additional locations in the future.

8.6 Interfaces

***Table 8.6-1**: Interfaces for the Test Cell Radiation Monitoring System (SBS 1.7.3.7)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
0.1.1.3	PPPL Network Infrastructure	Ethernet	At network switch	Radiation area monitors are network connected devices	N/A
1.8.1.1.4	NTC Walls	Structural	At NTC wall	Radiation area monitors mounted to wall.	General Arrangement Drawing
1.5.1.2	D-Site Auxiliary Power	Electrical Power	wall plug	Electrical power for radiation area monitors	N/A
1.8.1.1.5	NTC Penetrations	Spatial	At the penetration	Signals that enable area monitors to illuminate the radiation warning sign pass through penetrations in the NTC wall	N/A
1.8.1.3	North and East Galleries	Location	N/A	Radiation warning signs are located in the galleries near the test cell entrances	N/A

9: Test Cell Oxygen Deficiency Monitor

9.1 Functions

a. The function of oxygen monitors are to provide a visual and audible alarm to employees in the NSTX-U test cell and adjacent areas if an oxygen deficiency[4] situation exists in the test cell.

Note: Oxygen monitors located in other areas of the D-Site complex area are not described by these requirements, which are limited to the test cell and east gallery.

9.2 Materials and Design Requirements

a. Design, documentation, drawings, and labeling associated with this system shall be done consistent with the use of this system as a credited control under the accelerator safety order (ASO) [5,6].

b. The design shall be guided by ISA–RP92.04.02, Part II–1996 (R2013) *Installation, Operation, and Maintenance of Instruments Used to Detect Oxygen-Deficient/Oxygen-Enriched Atmospheres*

9.3: Configuration Requirements and Essential Features

a. Oxygen monitor points shall be located at four locations:

- Underneath the machine in the vicinity of Bays A/L

[4] An oxygen deficiency is defined as occurring if the oxygen concentration in monitored areas falls beneath 19.5%

- Elevated in the NTC in order to detect He at the elevation of the crane cab
- In the NTC West Shield Door (TFTR movable shield door) pit
- Near the LN2 fill station in the northeast corner of the gallery
- Amongst the HVEs on the north side of the test cell (near the floor)

b. This requirement voided.

c. Unless otherwise stated, monitor points shall be located at or below five feet from the floor to approximate average human breathing zones.

d. The ODH monitors shall have battery backup capability of at least 1 hour.

e. The ODH monitors shall be capable of detecting a low oxygen level regardless of the gas mixture.

f. The monitors shall not be affected by magnetic or radiation fields or shall be capable of being mounted outside the test cell.

g. All remote Status/Alarm indicators mounted inside the NTC shall be electrically isolated from the electronics mounted outside the test cell with isolation as per the GRD [1].

h. Connections between air sampling sensors and measurement components shall be routed and located in such a manner as to report oxygen deficiencies as efficiently as possible (shortest route).

i. The system shall have redundant ODH monitors for each location.

j. This requirement voided as of Rev. 2..

k. The system shall have remote status/alarm indicators mounted outside the test cell at the two personnel access doors and the two movable shield doors to alert personnel not to enter the test cell.

l. The system shall have remote status/alarm indicators mounted inside the test cell.

9.4 Baseline Performance and Operational Requirements

a. All remote Status/Alarm indicators shall annunciate when either monitor detects the oxygen level is at or below 19.5% oxygen.

b. Audible alarms shall be loud enough that personnel at any location within the NTC, including at entrances, will be able to clearly resolve the alarm above the background noise level.

9.5 Upgrade Performance and Operational Requirements

a. Additional sampling locations may be requested in the future, as the facility capabilities and equipment evolve.

9.6 Interfaces

Table 9.6-1: *Interfaces for the Test Cell Oxygen Monitoring System (SBS 1.7.3.11.1)*

Interfacing SBS	Interfacing System	Nature of Interface	Interface Boundary	Interface Description	Required Interface Documentation
1.8.1.1.1	NTC Platforms	Structural	At platform	ODH monitor system suspended/supported from platform	Conduit Drawing
1.5.1.2	D-Site Auxiliary Power	Electrical Power	At panel or plug	AC power provided to oxygen monitor system	Electrical Schematic
1.8.1.1.5	NTC Penetrations	Wall/Floor Penetration	At penetration surface	ODH monitor tubes pass through penetrations in the test cell wall	Conduit Drawing
1.8.1.1.5	NTC Penetrations	Structural	At the wall surface	ODH monitor system suspended/supported from Test Cell Wall	Conduit Drawing
1.8.1.1.5	NTC Penetrations	Wall/Floor Penetration	At penetration surface	ODH monitor tubes pass through penetrations in the test cell wall	Conduit Drawing