National Spherical Torus eXperiment Upgrade

Chit Resolution Report for *Personnel Safety System*

March 2, 2020

NSTXU_1-7-3-1_CRR_chit_100 Rev 3

Prepared By: Joseph R. Petrella Jr. Digitally signed by Joseph R. Petrella Jr. Date: 2020.03.02 11:34:58 -05'00'

J. Petrella, PSS Cognizant Engineer

Reviewed By: Timothy N. Stevenson Digitally signed by Timothy N. Stevenson Date: 2020.03.03 13:13:51 -05'00'

T. Stevenson, OSS RE

Reviewed By: Yuhu Zhai Digitally signed by Yuhu Zhai Date: 2020.03.04 08:51:47 -05'00'

Y. Zhai, Project Engineer

Approved By: Robert Ellis Digitally signed by Robert Ellis Date: 2020.03.04 15:59:12 -05'00'

R. Ellis, Chief Engineer

Final Design Review

Chit Resolution Number	Description	Chit Number	Status
CR-OSS-24	Component Selection	PSSFDR24 PSSFDR25	Closed Closed
CR-OSS-25	Calculation	PSSFDR11 PSSFDR12 PSSFDR14	Closed Closed Closed
CR-OSS-26	Drawings	PSSFDR02 PSSFDR03 PSSFDR04 PSSFDR05 PSSFDR08	Closed Closed Closed Closed Closed
CR-OSS-27	Future Testing	PSSFDR09 PSSFDR15 PSSFDR16 PSSFDR17	Closed Closed Closed Closed
CR-OSS-28	Documentation	PSSFDR01 PSSFDR10 PSSFDR21 PSSFDR26 PSSFDR29	Closed Closed Closed Closed Closed
CR-OSS-29	Additional Scope	PSSFDR27 PSSFDR28	Closed Closed

Record of Changes

Rev.	Date	Description of Changes
0	June 17, 2019	Initial Release
1	January 17, 2020	Added PDR Chits and Resolution(s)
2	February 18, 2020	Added Select FDR Chits and Resolution(s)
3	March 2, 2020	Added Balance of FDR Chits and Resolution(s)

Table of Contents

CR-OSS-24 – Component Selection

Review	ID	Chit
FDR	PSSFDR24	Consider contacting Subject Matter Expert (SME) at NSLS-II (e.g. Bob Lee) with regard to their PSS door switch issues experienced during early stages of operations to garner any lessons learned that might be valuable.

Closed: Bob Lee was contacted regarding NSLS-II door switch issues for lessons learned and the team reviewed the root cause report regarding the same. Switch failure occured due to the mechanical overthrow of limit switches (using them outside their operable range). While the NSTX-U PSS design uses non-contact switches on doors to avoid this issue, where limit switches are used the design mechanically limits the throw of limit switches to within their operable range thereby avoiding a similar failure mode. The NSLS-11 door switch issues were considered and were already addressed by the existing NSTX-U PSS design.

Review	ID	Chit
FDR	PSSFDR25	Consider the merits of evaluating the potential integrated radiological dose at the E-stop stations to inform predictions of of the LED stack light longevity if desired.

Closed: The NSTX-U PSS LED stack was designed to be easily testable (light test), modular (multiple LEDs per color), and readily serviceable (twist-off replacement with no tools). This reduces the need and benefit of performing a complex radiological study on the lifespan of easily testable and replaceable LED modules. The merits were considered and the benefits were not sufficient to warrant the expense of the study.

CR-OSS-25 – Calculation

Review	ID	Chit
FDR	PSSFDR11	Revisit FTA for NB operation and coils (boolean "AND" or "OR"?) for creating ionizing radiation.
FDR	PSSFDR12	Augment the assumptions basis portion of the LOPA calculation to include the references described during the presentation on the operator error frequency.

FDR	PSSDR14	SIL must meet the architectural constraints identified in the standards. The architectural constraints should be identified in the safety system specification, and associated with the SIFs.

Closed: The FDR calculation revision NSTXU_1-7-3-1_CALC_100, R0 was revised (new file NSTXU_1-7-3-1_CALC_100, R1) to incorporate updates to the Fault tree analysis (PSSFDR11) as well as the insertion of the reference for operator error (PSSFDR12). The Fault Tree Analysis in conjunction with the LOPA establishes the architectural constraints as noted in the minimum hardware fault tolerances contained illustrated within the PSS requirements document NSTX-U-RQMT-SRD-012.

CR-OSS-26 – Drawings

Review	ID	Chit
FDR	PSSFDR02	The loop diagram representation of the BCS for breaker tripping is misleading. The BCS does not make use of the 52UVD for tripping the breakers. The loop diagram drawings for the breakers should be changed to show a parallel connection to the breaker through the BCS for initiating a trip (trip coil of the breaker).

Closed: The loop diagrams have been updated to note the BCS shunt trip coil as well as to clarify the 125 VDC control power supply.

Review	ID	Chit
FDR	PSSFDR03	It is my understanding that CMS is for contact hazards, not "action at a distance" hazards. On that basis, the magnetic field labels should be removed from the CMSs

Closed: The magnetic hazard label has been removed from the label drawing D-AE8011.

Review	ID	Chit
FDR	PSSFDR04	Specify the dimensions of a clear space that needs to be covered to prevent personnel from passing between restricted areas.

Closed: A maximum safeguard opening has been defined and illustrated in NSTX-U-RQMT-SRD-012.

Review	ID	Chit
FDR	PSSFDR05	You may want to consider a different color for the "Configuration Managed Safeguard" label. White label is rather benign in appearance. At JLab all Critical Devices (such as movable radiation shielding, PSS interlocked doors and gates, etc.) are labeled using orange stickers to indicate that they are part of credited control.

Closed: All labels used for advisory purposes will follow the color scheme denoted in ANSI Z535. Notice labels with white backgrounds will be replaced with orange backgrounds, in accordance with the “warning” color scheme in ANSI Z535.

Review	ID	Chit
FDR	PSSFDR08	Consider adding on loop diagram symbols drawing explanation of additional acronyms used for PLC I/O ("TOP", "TOW", etc.?)

Closed: A description of terminology, acronyms, and symbols are included in Drawing D-AE8101. A note illustrating the location of these descriptions has been added to each loop diagram drawing.

CR-OSS-27 – Future Testing

Review	ID	Chit
FDR	PSSFDR09	Recommend to add Fiber Optic Failure Alarm Test to PLC Test Procedure
FDR	PSSFDR15	Test procedures for evaluation of the software have to be exhaustive.
FDR	PSSDR16	The software specification should be based on the system requirements, the system test should be based on the system requirements such that the software is shown to conform to the requirements. Software functionality that is in addition to the system requirements should be identified and tested. Negative functionality tests should prove that the software does not perform unexpectedly under normal operating conditions. Some subset of functional testing may only be required during initial testing and will not need to be performed after the software is found to be acceptable. These tests should be contained in a supplemental test procedure that is archived for future reference.
FDR	PSSDR17	Safety Instrumented Functions - Software Design, Testing and Functionality. General comment related to the presentation and more specifically to Slide 12. Has a Single Point Failure (SPF) been

		considered for each of the safety functions and related signal processing to ensure that one signal would not cancel the reporting or action of another single. In addition, it is understood that there is redundancy in the hardware (A&B) and therefore SPF is unlikely unless there is some type of software diagnostic that can be run to catch SPF reporting. Recommend a discussion on SPF in both hardware and software configurations.

Closed: Note these are not design-driving CHITs and are suggestions on testing regimens that will be reviewed separately from the design review process under laboratory procedure ENG-030. The suggestions included in these CHITs are accommodated by the draft testing procedures and will be not only verified/validated through ENG-030 review but also independently during the Stage 2 and Stage 3 Functional Safety Assessments.

CR-OSS-28 – Documentation

Review	ID	Chit
FDR	PSSFDR10	Confirm that 'Air Gap' of communications will satisfy the IEC 62443 standard for Industrial Cyber Security

Closed: This concern was previously raised and closed in the CDR chit resolution report:

CDR PSSCDR43 Ensure that cyber security approach conforms to IEC 62443

Closed: The NIST Guide to Industrial Control System Security (NIST.SP.800-82r2) cited in our cyber security requirements specifically calls out IEC 62443, entitled "Security for industrial process measurement and control –Network and system security." as one of the resources used to develop the guide. Further alignment with IEC 62443 those requirements will be reviewed as the software requirements are created.

Review	ID	Chit
FDR	PSSFDR01	Comment - Design Review Presentation - Terminology I'm in agreement with Dave Freeman's question and concern that the use of terminology associated with "credited" systems is confusing. In addition, explanation or definition of the terms "Safety Instrumented Function" (SIF) and "Safety Integrity Level/s" (SIL) needs to better understood in there relationship to Accelerator Safety Requirements or Accelerator Safety Envelope.
FDR	PSSFDR21	The PSS will serve as a "Credited Control" as defined in DOE O 420.2C. Consider the merits of clearly identifying the specific PSS functions that serve as the Credited Control (i.e. "credited functions")

		and clearly identify the PPS functions that provide other layers of "non-credited" safety.

Closed: Note these are not design-driving CHITs and are suggestions on documentation clarity that reach beyond the scope of the PSS. The PSS functions that are IEC-based SIFs are clearly identified in the PSS requirement documentation. In addition, PSS functions that are not IEC-based SIFs are delineated as 'additional engineering actions' per IEC standards. Due to the dual-perspective/definition of "credited" between IEC and the accelerator community, the accelerator-based "credited" distinction is made in the NSTX-U SAD document. The NSTX-U SAD will be the principle reference for accelerator community review and does not drive design basis (it is a reflection of design). The IEC-basis was leveraged to drive design therefore is used in the PSS design requirements.

Review	ID	Chit
FDR	PSSFDR26	Consider if using the term "trapped key" to refer only to Fortress keys might lead to confusion as Kirk keys are also used and are also considered "trapped keys". If confusion might exist, determine if improvement in nomenclature might be merited.

Closed: Note this is not a design-driving CHIT and is a suggestion on documentation clarity that reaches beyond the scope of the PSS. The existing Kirk Key system is used lab-wide and is entirely referenced as a "Kirk Key System". The "Trapped Key System" references a specific system within PSS and has limited scope to NSTX-U. Confusion, if any, would be an outcome of unfamiliarity with the system upon initial orientation. This potential confusion has no impact on system reliability or use, as individuals using the system must be trained prior to interaction with the system(s). The merit of renaming the Trapped Key System was considered by virtue of this chit and the limited benefits were not sufficient to warrant further consideration.

Review	ID	Chit
FDR	PSSFDR29	Add a Lamp / buzzer test function to SW req RD-100

Closed: A lamp/buzzer test was added to the software requirements document NSTXU_1-7-3-1-1_RD-100.

CR-OSS-29 – Additional Scope

Review	ID	Chit
FDR	PSSFDR27	Consider ways to mitigate pinch hazards that are inherent with the north shield door using appropriate engineered and/or administrative controls.

Closed: While this falls outside the scope of PSS as it pertains to a shield door not under the design purview of PSS, the concern can be addressed in this report. While the north shield door is large/heavy to operate, it is only operated by a limited group of specially trained machine technicians. The appropriate administrative controls (training, job hazard analysis) adequately addresses the potential hazards associated with operating the north shield door in accordance with laboratory ISM policies & procedures. The merit of the CHIT was considered and were not sufficient to warrant further consideration.

Review	ID	Chit
FDR	PSSFDR28	Consider the merits of erecting controlled personnel barriers within the test cell to establish areas that would not have to be re-swept unless entered should simplification of the search and secure process be desired.

Closed: Walkdowns of the search and secure path have been performed with machine technicians (search & secure team) to assess total search duration. It was determined that the theoretical incremental reduction in search time gained by segmenting the search areas was de minimis compared to the administrative and design complications introduced by the segmentation. The NSTX-U test cell complexity warrants a comprehensive search & secure process upon transition from an Access State to a No Access State. The merit of the CHIT was considered and were not sufficient to warrant further consideration.

Appendix 1 - Previous Rev 0 Chit Resolution Report

Chit Resolution Report for Personnel Safety System

Chit resolution report: NSTXU_1-7-3-1_CRR_chit_100

REVISION 0

July 12, 2019

PREPARED BY:	**Kathleen Lukazik**	6/20/2019 4:31:46 PM
	Kathleen Lukazik,	
REVIEWED BY:	**Joseph Petrella**	6/24/2019 7:20:18 AM
	Joseph Petrella,	
REVIEWED BY:	**Peter Dugan**	7/2/2019 11:17:26 AM
	Peter Dugan,	
REVIEWED BY:	**Timothy N. Stevenson**	7/2/2019 12:10:08 PM
	Timothy N. Stevenson,	
APPROVED BY:	**Stefan Gerhardt**	7/12/2019 1:36:55 PM
	Stefan Gerhardt,	

PRINCETON PLASMA PHYSICS LABORATORY
P.O. BOX 451
PRINCETON, N.J. 08543

National Spherical Torus eXperiment Upgrade

Chit Resolution Report for *Personnel Safety System*

June 17, 2019

Prepared By: _____
J. Petrella, PSS Cognizant Engineer

Reviewed By: _____
T. Stevenson, OSS RE

Reviewed By: _____
Y. Zhai, Project Engineer

Approved By: _____

DVVR

Chit Resolution Number	Description	Chit Number	Status
CR-OSS-05	E-Stops	TCACS02,	Closed
CR-OSS-07	Configuration	TCACS05	Closed
CR-OSS-09	Design	TCACS01	Closed
CR-OSS-12	E-Loop	TCACS04	Closed

NTC Shielding PDR

Chit Resolution Number	Description	Chit Number	Status
CR-OSS-05	E-Stops	NTCSHIELDPDR01	Closed
CR-OSS-06	Search and Secure	NTCSHIELDPDR08	Closed
CR-OSS-07	Configuration	NTCSHIELDPDR07	Closed

Conceptual Design Review

Chit Resolution Number	Description	Chit Number	Status
CR-OSS-01	Safety Integrity Level	PSSCDR01, PSSCDR04	Closed
CR-OSS-02	Hazards	PSSCDR02, PSSCDR03, PSSCDR05	Closed
CR-OSS-03	Requirements	PSSCDR06, PSSCDR07, PSSCDR08, PSSCDR09, PSSCDR11, PSSCDR15, PSSCDR17, PSSCDR20, PSSCDR28, PSSCDR29,	Closed

		PSSCDR30, PSSCDR32, PSSCDR33	
CR-OSS-04	Standards	PSSCDR36, PSSCDR43, PSSCDR44	Closed
CR-OSS-05	E-Stops	PSSCDR10, PSSCDR42	Closed
CR-OSS-06	Search and Secure	PSSCDR16, PSSCDR18, PSSCDR19,	Closed
CR-OSS-07	Configuration	PSSCDR41	Open
CR-OSS-08	Cost/Risk Reduction	PSSCDR31, PSSCDR34,	Closed
CR-OSS-09	Design	PSSCDR12, PSSCDR13, PSSCDR14, PSSCDR24, PSSCDR25, PSSCDR26, PSSCDR27, PSSCDR37, PSSCDR39	Closed
CR-OSS-10	Fail-Safe	PSSCDR23, PSSCDR35, PSSCDR40	Closed
CR-OSS-11	Policy	PSSCDR38	Closed
CR-OSS-13	Cable Spread Room	PSSCDR21	Closed

Peer Review

Chit Resolution Number	Description	Chit Number	Status
CR-OSS-14	Arc Flash	PSSPEER01	Closed
CR-OSS-15	NFPA 101	PSSPEER02	Closed

Record of Changes

Rev.	Date	Description of Changes
0	June 17, 2019	Initial Release

Table of Contents

CR-OSS-01 – Safety Integrity Level (SIL)

Review	ID	Chit
CDR	PSSCDR01	The term "SIL" is used incorrectly throughout documents. SIL is a failure on demand performance requirement for a system executing safety instrumented functions (SIF). Recommend having expert explain IEC61511 (61508) and how safety functions and ensuing SIL requirements are applied to your systems then revise documents to use SIF, SIL, and IPL correctly.

Closed: A SIS expert has been retained and has been consulted on IEC61511 aspects of the design. AE Solutions has been retained to perform third-party evaluations and verification of PSS-SIS capability.

Review	ID	Chit
CDR	PSSCDR04	Reconsider SIL decrement numbers. Administrative controls like radiation protection program are not a factor of 1000. Decrement is typically limited to a factor of 10 at the most.

Closed: Administrative controls and risks mitigated by Labwide Safety Programs have been removed from the PSS-SIS LOPA analysis. Labwide safety programs (such as the radiation protection program) are not part of the Safety Instrumented System and accordingly are not assigned risk reduction factors per IEC61511 guidelines.

CR-OSS-02 - Hazards

Review	ID	Chit
CDR	PSSCDR02	Under hazards, Radiation take away X-Ray and reference prompt radiation from secondary nuclear reactions

Closed: In consultation with ES&H all references to exclusion area radiation hazards that are mitigated by the PSS-SIS have been clarified to be “Direct Ionizing Radiation” and other hazards identified in the Hazard assessment Report (HAR).

Review	ID	Chit
CDR	PSSCDR03	Include stray magnetic field and vacuum in list of hazards to be assessed.
CDR	PSSCDR05	Vacuum related hazards should be considered. Not listed in presentations.

Closed: The HAR (NSTX-U-DOC-123-00) that was developed post-CDR addresses all industrial hazards including magnetic field and vacuum hazards.

CR-OSS-03 - Requirements

Review	ID	Chit
CDR	PSSCDR06	Consider making enclosure audible and visual warnings as a credited control. Need to let someone know it is time to push ESTOP.
CDR	PSSCDR32	Audible & Visual warnings should be credited control

Closed: The SRD NSTX-U-RQMT-SRD-012-01 Requirement 3.1.1.e was updated to move audible and visual warning to credited controls as part of the SIS.

Review	ID	Chit
CDR	PSSCDR07	Consider changing word "mode" to "state" for the description of the PSS states. This is to differentiate from test modes.

Closed: The SRD NSTX-U-RQMT-SRD-012-01, RD-24 NSTX-U-RQMT-RD-024-01 have been updated to ensure that only states of ACCESS and NO ACCESS, LOCKED are identified all other references have been changes to modes.

Review	ID	Chit
CDR	PSSCDR08	Consider to define time requirement from when PSS is in "No Access" state to when the hazards are permitted to be "applied".

Closed: The NSTX-U-RQMT-SRD-012-01 was updated to include a time delay of at least 300 seconds between change to NO ACCESS state to when hazards can be applied is defined in Performance Requirements 3.4.b.

Review	ID	Chit
CDR	PSSCDR09	Consider modes where the sweep is in place but beam is not allowed, e.g. after a radiation monitor trip. Some labs call this "Power Permit"; certain devices are ok to run, e.g. magnet power supplies and/or RF power. Also mode where warnings active but beam not enabled.

Closed - Not Applicable: The Beams are not steerable as a result there are no interlocks to the radiation monitor.

Review	ID	Chit
CDR	PSSCDR11	Consider using words clearly describing PSS states like: OPEN, SWEEP, RUN, LOCKED.

Closed: Considered the Chit, but it was rejected to maintain the three states: Access, No Access, Locked. The currents states are tracked as either access or no access. There is a future requirements to consider other states. As additional states, are added additional states can be added.

Review	ID	Chit
CDR	PSSCDR15	Should the RF coax be monitored by PSS? I was told these are pressurized, pressure gauge will be read, but there is not intention to monitor them by PSS.

Closed - Not Applicable: This is not a personnel safety concern as there is no personnel safety impact if the RF transmission lines would become de-pressurized. The RF transmission line pressure is a machine protection and control function and it is already incorporated into the operational control of the RF systems.

Review	ID	Chit
CDR	PSSCDR17	Should indicated "LOCKED" in the area status panels.
CDR	PSSCDR30	Locked mode should have an indicator that the area is locked down.

Closed: RD-24 NSTX-U-RQMT-RD-024-01 has been updated to include the Locked Mode for securable areas. Locally, visual indicators will only state “Access” and “No Access” with “No Access” mapped to both No Access and Locked states.

Review	ID	Chit
CDR	PSSCDR20	To avoid stationing guard at the entry door to the Secure Area, you can provide to CCS control over the door maglock to keep the door locked while the S&S is in progress.

Closed: Added a best practice in RD-24 Section 3.3.3.f versus a requirement to monitor the status of trapped keys. The SIS will locally disable the card readers on doors to securable areas during S&S. An additional TKS locked vestibule will prevent individuals from approaching the second entryway into the NTC.

Review	ID	Chit
CDR	PSSCDR28	Monitor Trapped keys with PSS
CDR	PSSCDR29	Should monitor the state of the trapped key to insure presence of the key

Closed: The PSS-SIS will not monitor the Trapped Key System. Rather, the Trapped Key system is monitored by the CCS as defined in RD-026 Section 3.3 and displayed in the control room.

A requirement was added for as part of access control Section 3.3.2.k to monitor the status of the PSS.

Review	ID	Chit
CDR	PSSCDR33	Recommend against a local test button that injects signal into a PLC controlled status lamp. Lamp test could be controlled through the PLC HMI.

Closed: The requirements in RD-24 Section 3.8.1.n for a local lamp-check button have been removed and this function is recommended to be performed via the PLC HMI.

CR-OSS-04 - Standards

Review	ID	Chit
CDR	PSSCDR43	Ensure that cyber security approach conforms to IEC 62443

Closed: The NIST Guide to Industrial Control System Security (NIST.SP.800-82r2)

cited in our cyber security requirements specifically calls out IEC 62443, entitled "Security for industrial process measurement and control –Network and system security." as one of the resources used to develop the guide. Further alignment with IEC 62443 those requirements will be reviewed as the software requirements are created.

Review	ID	Chit
CDR	PSSCDR44	Ensure that SIS PLC Configuration conforms to IEC 61131

Closed: We will ensure conformance with IEC61131 through our PSS Software requirements and Software Quality Assurance (SQA) software management plan. This plan is required per PPPL's QA028 procedure outlining requirements for SQA.

Review	ID	Chit
CDR	PSSCDR36	1. Should Quality Assurance requirements (e.g. Order 414) be identified as a driver for PPS design, installation, operations, maintenance, etc? Is there a driver for a QA Plan that would address Credited Controls including the PPS?

Closed: The PPPL QAPD describes implementation of, and compliance with, DOE O 414 at PPPL. The PSS is identified as an A-1 system per ENG-032, in accordance with the PPPL QAPD and has had the applicable quality controls applied to it. PSS-SIS has been identified as a Credited Control system. Management of Credited Controls will be described in the NSTX-U SAD, which is currently undergoing substantial revision to comply with DOE O 420.2C.

CR-OSS-05 - E-Stops

Review	ID	Chit
CDR	PSSCDR10	"Equipment-specific local E-Stop push buttons must be functionally segregated from the PSS E-STOP". Make sure they are not mistaken with PSS E-Stops.

Closed: NSTX-U PSS E-Stops have been designed to be visually unique and are clearly labeled. NSTX-U PSS E-Stops are installed on Search & Secure Stations, including those for control and status. These stations have "NSTX-U E-STOP" engraved in large bold letters, and the boxes are easily identifiable; their front panels are marked with a white on purple color scheme unique to PSS and have a multicolor indicator beacon on top.

Review	ID	Chit
CDR	PSSCDR42	It appeared more work is needed to finalize the locations of the E-stop/search stations. Consider establishing some documented guidance and identifying key staff to be involved in physically walking down the areas to determine specific locations. Key staff might include personnel with significant experience conducting search/sweeps, the radiation safety officer (or equivalent), and individuals responsible for installing the E-stop/search stations.

Closed: The locations of the NSTX-U PSS S&S Stations and E-Stops have been mocked-up in the exclusion areas. The design and location of these stations have been reviewed and walked-down by the appropriate senior technicians who perform the search & secure process and subject matter experts. These walkdowns resulted in movement and addition of some stations.

Review	ID	Chit
Test Cell DVVR	TCACS02	The consequence of a false E-Stop during a shot can be dire in terms of damage to SDS cabinet components. Consider an assessment of false trips including i) blocking access to doors during operations, ii) redundant switches on doors, iii) other things that might prevent an errant e-stop...

Closed: Spurious trips have been addressed in multiple ways:

1) PSS-SIS monitored access doors are behind vestibule cage doors that are independently locked with the trapped key system to prevent access door challenges.
2) Safety capable components have exclusively been deployed in the monitoring and interdiction components ensuring a quantifiable level of reliability and determinable spurious trip rate.
3) A timing scheme has been designed for PSS-SIS so that existing BCS machine-protection systems operate first during a NSTX-U PSS E-Stop event to allow for the optimal shutdown of equipment. Only if the BCS fails to perform it's orderly shutdown does the PSS-SIS terminate interdiction devices.

Review	ID	Chit
NTC Shielding PDR	NTCSHIELD PDR01	Consider the need to install E-Stop buttons in the Basement MER and MER Mezzanine to allow someone to stop an NSTX-U shot if they have not evacuated these areas.

Closed: It was determined through the assessment of Direct Ionizing Radiation and other hazards identified in the HAR hazards that NSTX-U PSS E-STOPS would be installed in the MER Mezzanine. The MER Basement posed no Direct Ionizing Radiation risk and therefore no NSTX-U PSS E-Stops were required in that location.

CR-OSS-06 – Search and Secure

Review	ID	Chit
CDR	PSSCDR16	Should the S&S ready light be installed on the box? If you enforce the dropping the S&S state when out of order box is armed, why do you help the S&S crew in identifying which box is next?
CDR	PSSCDR19	Should the S&S ready light be installed on the S&S box? If you enforce the dropping the S&S state when out of order box is armed, why do you help the S&S crew in identifying which box is next? S&S crew should be well trained to perform the procedure.

Closed: Removed the ready light from the design, search crew will be trained in the prescribed path. This training will be added to operator training matrices per the NSTX-U Training & Qualification Program for the operators required to complete these evolutions.

Review	ID	Chit
CDR	PSSCDR18	Consider additional Search and Secure stations in the south high bay, particularly on the west side of that area.

Closed: Added to PDR design, this additional S&S Station also provides an E-Stop required by ESHD 5008 (50 ft. travel to an E-Stop).

Review	ID	Chit
NTC Shielding PDR	NTCSHIELD PDR08	Add search and secure stations to test cell requirements document.

Closed: Between SRD-12 OSS & SRD-24 PSS many requirements have been added for Search & Secure Stations.

CR-OSS-07 – Configuration

Review	ID	Chit
CDR	PSSCDR41	PSS Configured Items List, Components that are critical to system operation should be identified as critical with a "like for like" replacement strategy. Helps with replacement and analysis.

Open: The PPPL policy requires all components provide a like-for-like component replacement unless otherwise specified as equivalent. As part of the design leading towards FDR, specific critical components will be selected and included in the design.

Post FDR, if a critical component requires change that is not like-for-like an engineering change notice (ECN) will be generated. Since the design is ongoing his chit will remain open and be formally closed at FDR.

Review	ID	Chit
Test Cell DVVR	TCACS05	Some drawings related to the HIS may not be fully up to date (I am told). Since this is a human safety system, it seems to me like this may be one place where we need to ensure fully up to date documentation.
NTC Shielding PDR	NTCSHIELD PDR07	While this NTC updates HIS drawings where touched, a broader surveyed assessment of HIS drawing existence and accuracy is needed for the project

Closed: Drawings are being updated as needed to reflect PSS systems updates.

CR-OSS-08 – Cost/Risk Reduction

Review	ID	Chit
CDR	PSSCDR31	Add cost to develop SRSs & SIF test procedures to estimate.

Closed: These costs have been included in the revised WAF and were previously included in the FDR planning package.

Review	ID	Chit
CDR	PSSCDR34	Consider Basic Control System for Risk Reduction Credit.

Closed: It is acknowledged that IEC61511 permits applying a maximum Risk Reduction Credit of 10 to basic control systems. For conservatism the quantitative LOPA performed for PDR did not incorporate this Risk Reduction Credit in the generation of SIF performance requirements. However, this Risk Reduction Credit may be incorporated into the system performance calculations that will be performed for FDR. Accordingly the design team has considered, and will deploy if necessary, the allowed basic control system Risk Reduction Credit as part of the system performance calculations.

CR-OSS-09 –Design

Review	ID	Chit

CDR	PSSCDR12	Note that, whenever SLD line switches are closed and ground switches open, the hazard is present. Only the local controls and interlocks, not intended for a safety function, prevent the delivery of energy to the coils by control of the thyristor gate pulses. Moreover, even when the thyristors are not gated, there is voltage on the bus due to thyristor snubber paths. Therefore, the duty factor of pulsing should not be credited in the analysis.

Closed: This chit refers to the potential of electrical hazards on exposed buswork in the exclusion areas. As documented in the May 8, 2019 Peer Review, electrical hazards will be mitigated through Configuration Managed Safeguards and Laboratory Integrated Safety Management policies/procedures.

Review	ID	Chit
CDR	PSSCDR13	Confirm that Allen Bradley 440N door monitor switches are not susceptible to stray magnetic field

Closed: The location of the magnetic door monitoring switches are far outside the influence of stray magnetic fields in the test cell. This was verified by examining the distance to the machine centerline and magnetic field maps.

Review	ID	Chit
CDR	PSSCDR14	Please consider retaining the personnel door on the SHB labyrinth. Why? It can be used to slow access from the interlocked door to the more hazardous areas of the test cell. No need to retain the card reader, just the door.

Closed: The personnel door at the south high bay labyrinth has been preserved, sans card reader.

Review	ID	Chit
CDR	PSSCDR24	The Ross HV Divider is not a safety rated device. Consider implementing redundant dividers.

Closed: The Ross HV Divider for use in a Safety Instrumented Function has been eliminated in the PDR design.

Review	ID	Chit
CDR	PSSCDR25	For SV breaker interdiction, determine if tripping and status interface with PSS can be accomplished in ACDS control boards where the signals are already concentrated, to avoid running cable to individual SV breaker cubicles.

Closed: This suggestion was considered but rejected since it is required to have end-to-end IEC61511 compliant hardware/software for Safety Instrumented Function interdicted devices.

Review	ID	Chit
CDR	PSSCDR26 PSSCDR27	To avoid interdicting AC input via the numerous individual SV breakers, consider alternate solutions for E-stop such as 1) install new load-break type breakers on the input to each of the SV bus bars for PSS purposes, or 2) install new MG breaker(s) to replace the existing units which are at end of life.

Closed: As proposed in the May 8, 2019 peer review, specific breakers in the SV/SF lineup will be replaced in addition to the installation of a new S1-B1 breaker that is upstream of the SV/SF lineup. The replacement addresses adding an additional layer of interdiction (S1-B1), De-Energize-to-Trip undervoltage trip devices, and end-of-life concerns with the existing breakers.

Review	ID	Chit
CDR	PSSCDR37	Consider the merits of adding PPS features that help to enforce the configuration of access control barriers (e.g. moveable shielding, cage barriers (e.g. roofs), etc.

Closed: Configuration Managed Safeguards have been designed to augment PSS-SIS Safety Instrumented Functions in a complementary and independent way. For instance, a trapped-key-interlock will be installed on a vestibule cage door outside of exclusion area entrance doors so that individuals who are outside the exclusion area are unable to challenge the PSS-SIS monitored entry door. Safeguards that are part of the Configuration Managed Safeguards will be configuration controlled through design documentation, work permits, and dictums of the NSTX-U SAD.

Review	ID	Chit
CDR	PSSCDR39	Line-items in the final presentation listed Controllogic PLC - instead of Guardlogix

Closed: The Guardlogix product family is a component of the Controllogix family. Features such as chassis, power supplies, cabling, and communication modules are shared between the Guardlogix and Controllogix products. BOMs have been generated in accordance with the manufacturer's product manuals.

Review	ID	Chit
Test Cell DVVR	TCACS01	Consider reviewing a fault condition where a false high is present in the loop due to a 120V crossover. The concern is that the loop may not drop if a loop short to 120V occurs (through a cable issue etc). Consider running the hot and return wires for the loop through separate conduit or install redundant parallel loops that are run in separate conduits.

Closed: The design of the E-Stop 'loop' has substantially changed from the TFTR-era 120VAC single-wire E-Stop loop system. PSS-SIS features a home-run individual 24VDC continually pulse-diagnostic monitored circuit to each NSTX-U PSS E-Stop button. The notion of a single-loop exclusion area integrity circuit is also no longer applicable as PSS-SIS features a home-run individual 24VDC continually pulse-diagnostic monitored circuit to each door monitoring switch.

CR-OSS-10 -Fail-Safe

Review	ID	Chit
CDR	PSSCDR23	Assure that when you convert energy within SIS such as electrical to pneumatic, the selected devices or implementations conform to fail-safe philosophy.

Closed: A De-Energize-to-Trip philosophy has been adopted for all PSS-SIS Safety Instrumented Functions. The means of implementation have been documented and demonstrated during the May 8, 2019 Peer Review and in the Preliminary Design materials.

Review	ID	Chit
CDR	PSSCDR35	Shunt trip is not fail-safe, the removal of energy should signal the faulted condition and trigger an intervention. Motor driven switches are not fail-safe. There must be a device in the interlock chain that operates under the condition of loss of power. Ground switches are fail-safe, and interrupt hazardous power. Volume bottle does not provide a fail-safe energy source to the ground switches.

Closed: PSS-SIS will employ undervoltage trip releases on all interdicted breakers for Safety Instrumented Function actions and not shunt trips. There will be no motor driven switches used for Safety Instrumented Functions. It is presumed that 'Volume bottle' is meant to be 'Vacuum Bottle'. While opening a vacuum breaker is not considered to render a circuit electrically 'safe' in accordance with NFPA 70E, the purpose of opening such a breaker is to terminate the flow of significant current required for the generation of Direct Ionizing Radiation. For this purpose, vacuum bottle breakers are sufficient. Discussion of the use of vacuum bottle contactors/breakers and their acceptable use in

SIFs is documented in the article: *"Integrating switchgear breakers and contactors into a safety instrumented function"*, Grattan et. al. May 18, 2010, Journal of Loss Prevention in the Process Industries. The elimination of downstream electrical hazards per NFPA 70E are not part of a Safety Instrumented Function and are mitigated by Laboratory Integrated Safety Management policies/procedures.

Review	ID	Chit
CDR	PSSCDR40	Consider the merits of redesign such that all credited features of the PPS are failsafe. For example, the relay logic for a shunt trip is not fail safe. It is desirable that a foreseeable condition, such as a broken wire, would not be able to defeat the system.

Closed: Duplicate - PSSCDR23, PSSCDR35

CR-OSS-11 – Policy

Review	ID	Chit
CDR	PSSCDR38	Consider the merits of adopting an approved written policy to help guide consistent and appropriate labeling of PPS system components, conduit, etc.

Closed: The configuration management policies of the laboratory drive the application of PSS specific labeling; in addition, a specific PSS design has been developed as described in NSTX-U-DOC-127, "*Labeling, Identification, and Tamper Resistance for the NSTX-U Personnel Safety System*". This document describes the PDR level design and will be revised as necessary to support the FDR. PSS-SIS has been identified as a Credited Control system, and as such, they will be labeled in accordance with the NSTX-U credited control management program described in the SAD.

CR-OSS-12 – E-Loop

Review	ID	Chit
Test Cell DVVR	TCACS03	Status transition logic for E-loop. What happens when E-loop is broken during a pulse? Which transition occurs and what sequence of actions is taken?

Closed: The status transition is documented in the PSS-SIS software design timing architecture.

Review	ID	Chit
Test Cell DVVR	TCACS04	All E-loop knowledge with one person, combination of others covers part.

Closed: While this chit is not actionable, the implementation of the PSS has involved a large design team who share intimate knowledge of the updated NSTX-U PSS E-Stop design. All design aspects are being exhaustively documented for this new system. The system design knowledge does not reside with any single individual.

CR-OSS-13 – Cable Spread Room

Review	ID	Chit
CDR	PSS CDR21	Consider the Cable Spread Room as a lockable area since it is rarely accessed.

Closed: The cable spread room is not an exclusion area monitored by the PSS-SIS. Rather, it is secured and coordinated by the trapped key system.

CR-OSS-14 – Arc Flash

Review	ID	Chit
PSS Peer Review	PSSPEER01	Examine arc flash safeguards / CMS are adequate.

Closed: Informational Note 1 under the definition of Arc Flash Hazard in NFPA 70E 2015 (Standard for Electrical Safety In the Workplace) indicates: *An arc flash hazard may exist when energized electrical conductors or circuit parts are exposed or when they are within equipment in a guarded or enclosed condition, provided a person is interacting with the equipment in such a manner that could cause an electric arc. Under normal operating conditions, enclosed energized equipment that has been properly installed and maintained is not likely to pose an arc flash hazard.*

During dummy load testing, the PCTS is in a guarded state (completely enclosed by covers) and no personnel are interacting with the PCTS such that an electric arc could be initiated. Further detail is provided in memo ARC FLASH HAZARD OF THE POWER CABLE TERMINATION STRUCTURE (PCTS) DURING DUMMY LOAD TESTING, PWR-190605-JD-01.

CR-OSS-15 – NFPA 101

Review	ID	Chit
PSS Peer Review	PSSPEER02	Emergency exits from the NTC need to be compliant with NFPA 101.

Closed: Personnel doors from NTC have NFPA 101 compliant egress hardware. An exterior caged vestibule will have the TKS hardware installed on the cage door with single-motion COTS egress hardware installed. The final caged vestibule will be closed after NTC search & secure, however an individual present behind any closed/locked door will be able to egress with a single-motion outward swinging door. The configuration and hardware have been reviewed and approved by the onsite AHJ.

Appendix 2 - Previous Rev 1 Chit Resolution Report

National Spherical Torus eXperiment Upgrade

Chit Resolution Report for *Personnel Safety System*

January 17, 2020

NSTXU_1-7-3-1_CRR_chit_100 Rev 1

Prepared By: 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: 2020-01-17 08:15:57

J. Petrella, PSS Cognizant Engineer

Reviewed By: Timothy N. Stevenson — Digitally signed by Timothy N. Stevenson Date: 2020.01.21 09:36:38 -05'00'

T. Stevenson, OSS RE

Reviewed By: Yuhu Zhai — Digitally signed by Yuhu Zhai Date: 2020.01.17 08:26:26 -05'00'

Y. Zhai, Project Engineer

Approved By: John Dellas — Digitally signed by John Dellas Date: 2020.01.21 10:19:50 -05'00'

J. Dellas, DRC

Conceptual Design Review

Chit Resolution Number	Description	Chit Number	Status
CR-OSS-07	Configuration	PSSCDR41	Closed

Preliminary Design Review

Chit Resolution Number	Description	Chit Number	Status
CR-OSS-16	TKS & CMS Design	PSSPDR01 PSSPDR02 PSSPDR03 PSSPDR04 PSSPDR05 PSSPDR06	Closed
CR-OSS-17	SIS PLC Design	PSSPDR07 PSSPDR10	Closed
CR-OSS-18	Human Factors	PSSPDR08	Closed
CR-OSS-19	Cost & Schedule	PSSPDR09	Closed

Record of Changes

Rev.	Date	Description of Changes
0	June 17, 2019	Initial Release
1	January 17, 2020	Added PDR Chits and Resolution(s)

Table of Contents

CR-OSS-07 – Configuration

Review	ID	Chit
CDR	PSSCDR41	PSS Configured Items List, Components that are critical to system operation should be identified as critical with a "like for like" replacement strategy. Helps with replacement and analysis.

Closed: As part of the FDR design, critical components have been selected and included in the design documentation. Post FDR, if a critical component requires change that is not like-for-like an engineering change notice (ECN) and a unresolved safety issue (USI) will be generated. A draft Critical Component Specification plan has been generated and will be finalized prior to commissioning.

CR-OSS-16 – TKS & CMS Design

Review	ID	Chit
PDR	PSSPDR01	Consider adding the grounding cage interlock in the TFTR TCB. Particularly if it is intended to remove the junction area transfer station.

Closed: The grounding cage interlock has been incorporated into the TKS design (Ref AE8010).

Review	ID	Chit
PDR	PSSPDR02	Consider getting a full set of spare TKS keys for a variety of reasons

Closed: A full spare set of TKS keys are planned in the procurement of TKS keys.

Review	ID	Chit
PDR	PSSPDR03	Ensure that the 2nd floor RWM Kirk Key is accommodated for in TKS.

Closed: The RWM key interfaces with the TKS at a Kirk-Key to Fortress-Key transfer station located near the existing SLD (Ref D-AE8355_1).

Review	ID	Chit
PDR	PSSPDR04	Please include the SPA more explicitly in the requirements for TKS and CMS

Closed: SPA-1 has been incorporated into the FCPC electrical protection design (Ref 0AE8352_3) and will be locked with existing machine-protection Kirk-Keys as part of the existing FCPC operations Kirk-Key system.

Review	ID	Chit
PDR	PSSPDR05	Please include the SPA more explicitly in the requirements for TKS and CMS Monitoring of TKS should include appropriate CCS alarms when the key configuration is inconsistent or unsafe.

Closed: SPA-1 has been incorporated into the FCPC electrical protection design (Ref 0AE8352_3) and will be locked with existing machine-protection Kirk-Keys as part of the existing FCPC operations Kirk-Key system. TKS is monitored by both CCS and SIS for condition-of-plant and configuration. SIS monitores all systems for inconsistent states (Ref NSTX-U-RQMT-RD-025-1_CCS, NSTXU_1-7-3-1-1_RD_100_00_SIS).

Review	ID	Chit
PDR	PSSPDR06	The maturity of the trapped key design is well below that of the electrical safety systems. E.g. not even red-line diagrams were presented. I would not consider the trapped key design at the PDR level.

Closed: This chit was rejected by the PDR Design Review Chair (Ref NSTXU_1-7-3-1_PDRs_100).

CR-OSS-17 – SIS PLC Design

Review	ID	Chit
PDR	PSSPDR07	I strongly recommend using two separate DC power supplies – one for chain A and one for B. High, low, and noisy power is a known common cause failure mechanism for PLCs and IO. If you still want to go with one supply, at least monitor the power supply fault contacts.

Closed: Redundant power supplies are used in the control cabinet design and power supply alarms are monitored by the control system.

Review	ID	Chit
PDR	PSSPDR10	Perform analysis for any instrument failure before proceeding with like-for-like replacement

Closed: The spirit of this chit has been incorporated into the draft Critical Component Specification Plan: *"An instrument failure analysis shall be performed if replacement is required due to component failure. The mode of failure shall be evaluated and incorporated into the determination of the proper replacement component and if required shall trigger a design review to ensure proper operation."* The plan is at a draft state at FDR and will be finalized prior to commissioning. The plan does not impact the final design of the system and is only applicable after commissioning of the system.

CR-OSS-18 – Human Factors

Review	ID	Chit
PDR	PSSPDR08	The project should address human factors to include operator interfaces and alarms at this stage. This may affect things like tags and tag properties, fault diagnostics and testability, and disambiguation.

Closed: Tag construction, alarms, and human machine interfaces are defined in the software requirements document NSTXU_1-7-3-1-1_RD_100.

CR-OSS-19 – Cost & Schedule

Review	ID	Chit
PDR	PSSPDR09	Also schedule needs to include labor for independent review of both hardware and software. Include any tools needed, e.g. RS5000 to review and compare software. Should include at least one iteration.

Closed: The PSS-SIS work packages include Stage 2 and Stage 3 functional safety assessments and supporting M&S.

Appendix 3 - Previous Rev 2 Chit Resolution Report

PRINCETON PLASMA PHYSICS LABORATORY

ENG-033 - CRR - CHIT RESOLUTION REPORT

CHIT RESOLUTION REPORT FOR PERSONNEL SAFETY SYSTEM

NSTXU_1-7-3-1_CRR_100

Rev. 2

Work Planning #:
Effective Date: **02/20/2020**
Prepared By: **Joseph Petrella**

Approved By Kathleen Lukazik, Preparer 02/20/2020 13:02:25 PM

PRINCETON PLASMA PHYSICS LABORATORY
P.O. BOX 451 PRINCETON, N.J. 08543

National Spherical Torus eXperiment Upgrade

Chit Resolution Report for *Personnel Safety System*

February 18, 2020

NSTXU_1-7-3-1_CRR_chit_100 Rev 2

Prepared By: Joseph R. Petrella Jr. Digitally signed by Joseph R. Petrella Jr. Date: 2020.02.18 14:56:10 -05'00'

J. Petrella, PSS Cognizant Engineer

Reviewed By: Timothy N. Stevenson Digitally signed by Timothy N. Stevenson Date: 2020.02.19 10:13:23 -05'00'

T. Stevenson, OSS RE

Reviewed By: Yuhu Zhai Digitally signed by Yuhu Zhai Date: 2020.02.19 10:58:56 -05'00'

Y. Zhai, Project Engineer

Approved By: Robert Ellis Digitally signed by Robert Ellis Date: 2020.02.19 18:10:36 -05'00'

R. Ellis, Chief Engineer

Chit Resolution Number	Description	Chit Number	Status
CR-OSS-20	Rejected Chit	PSSFDR06	Rejected at FDR
CR-OSS-21	Conduit Design	PSSFDR07 PSSFDR18 PSSFDR19 PSSFDR20	Closed Closed Closed Closed
CR-OSS-22	General Design/Drawings	PSSFDR13	Closed
CR-OSS-23	Control Cabinets	PSSFDR22 PSSFDR23	Closed Closed
CR-OSS-24	Component Selection	PSSFDR24 PSSFDR25	Closed Closed

Record of Changes

Rev.	Date	Description of Changes
0	June 17, 2019	Initial Release
1	January 17, 2020	Added PDR Chits and Resolution(s)
2	February 18, 2020	Added Select FDR Chits and Resolution(s) for conduit installation

Table of Contents

CR-OSS-20 – Rejected

Review	ID	Chit
FDR	PSSFDR06	Combine signed calculation PDFs to fix DMS truncation of the filed calculation.

Closed: This chit was rejected by the DRC at the FDR due to the fixed calculation being assembled and uploaded to DMS prior to the completion of the FDR.

CR-OSS-21 – Conduit Design

Review	ID	Chit
FDR	PSSFDR07	Revisit need for spare cables to FCPC SDS cabinets, some may be unnecessary.
FDR	PSSFDR19	Conduit & cabling located in FCPC associated with the EF/VC-SDS and EF/OH disconnect switch is not required. These cabinets will not be brought online for the life of NSTX-U

Closed: Spare conduit/cables in FCPC to equipment not envisioned to be needed in the near future were removed from the drawing set.

Review	ID	Chit
FDR	PSSFDR18	Consider adding additional references on drawings when installing new devices in existing equipment.
FDR	PSSFDR20	All PSS-SIS drawings shall reference existing PPPL drawings where applicable.

Closed: Pre-existing reference drawings, where applicable and available, were added to the conduit/cable drawing set.

CR-OSS-22 – General Design/Drawings

Review	ID	Chit
FDR	PSSFDR13	Generalized drawings of common hardware is a good practice and reduces redundant drawings that may be similar and confusing. Identifying mark on physical hardware should match reference tables on generalized drawing.

Closed: Hardware identification is included in the presented design at FDR and is located in the notes on completed drawings.

CR-OSS-23 – Control Cabinets

Review	ID	Chit
FDR	PSSFDR22	Consider the merits of evaluating the heat load in PSS cabinets to ensure components are maintained below manufacturer specifications under all credible load conditions. Note that cabinet heat loading has led to performance issues at some peer facilities.
FDR	PSSFDR23	Consider the merits of designing PSS cabinets with sufficient passive cooling to maintain temperatures below manufacturer specifications such that active cooling is not essential for operability.

Closed: Cabinet volumes and rack-ups were selected in accordance with COTS component manufacturer specifications. The use of in-field (outside of control cabinets) interposing relays in the design minimizes the switched load in each control cabinet. As an assurance measure each cabinet design will be evaluated by the cabinet builder for heat load performance as part of the outsourced cabinet design detail & fabrication procurement.