

**SNS-OPM-ATT 2.B-10.a.  
Unreviewed Safety Issue (USI) Evaluation Form**

**I Title of USI Evaluation:**

**Modifications to the TPPS to resolve the Primary Shutter Reopening Abnormality and removal of the Maintenance Key Switches.**

**II Description of Proposed Activity (or discovered condition):**

This USI evaluates two proposed modifications to the Target Personnel Protection System (TPPS) hardware and PLC logic. Both modifications concern TPPS functionality for the monitoring and control functions for dual beamlines, i.e. instrument beamlines that share one Primary Shutter.

- a. Modification 1 is to address an error in the functionality of the Primary Shutter OPEN controls for beamlines 1A/1B and 11A/11B. The anomaly allowed the Primary Shutter OPEN command to go through even if one of the two beamlines has an active fault.<sup>1</sup> The PPS would detect the shutter starting to open then re-issue the CLOSE command.<sup>2</sup>  
A temporary modification in July 2014 used hardwired relays to prevent opening the beamline 1 and 11 Primary shutter if one of the two instruments on each line asserted a fault condition. The hardwired modification will be removed and the TPPS PLC A logic modified to inhibit the primary shutter OPEN command if there is a fault in either of two dual beamlines. The modification will be for all dual beamlines. This modification affects TPPS division A only because the division A PLC issues the primary shutter OPEN command.
- b. Modification 2 is to remove a maintenance mode function originally intended to augment the administrative bypass of one dual beamline instrument while the partner beamline remains online. This functionality is part of the documented baseline TPPS design; however the function has never been used and is viewed as a vulnerability in the TPPS configuration management. Modification 2 affects both TPPS Division A and Division B hardware and software for all dual beamlines.

The two proposed modifications do not directly affect the TPPS safety functions described in the FSAD and ASE. Rather, they make the TPPS implementation more robust and resilient against errors in operations and configuration management.

**II.A Summary of Changes to TPPS Hardware and Software**

Technical specification 109090200-TS0001 describes the detailed changes to hardware and PLC program (software) required to effect the proposed changes. The PLC program modifications will be implemented as part of the CCR Rack Replacement project (see USI 102030102-ES0080 R00).

- 1) Modifications to TPPS PLC Logic for primary shutter reopening abnormality
  - a) Modify the TPPS PLC A logic to add a condition to inhibit the “Primary Shutter Open” command if there are faults from either IPPS on a dual beamline.

---

<sup>1</sup> See USI 102030102-ES0075

<sup>2</sup> The credited safety function for protection of an instrument is to shut off the front end. Operation of the Primary Shutters is a non-credited function.

- b) Remove relays K1, K2 and their associated wiring from TPPS PLC cabinet PPS\_TGT: CAB05. These relay contacts are used to interrupt the primary shutter open command push button input signal for BL-1A.
  - c) Remove relay K1, K2 and their associated wiring from TPPS PLC cabinet PPS\_TGT: CAB07. These relay contacts are used to interrupt the primary shutter open command input signal for BL-11B.
- 2) Removal of the Target PPS (TPPS) “maintenance key” mechanisms
- This change affects the TPPS safety functions monitoring dual beamlines only. Dual beamlines are those with two instruments sharing one primary shutter. The planned and operational dual beamlines are: (1A/1B, 4A/4B, 8A/8B, 11A/11B, 14A/14B, and 16A/16B).
- a) Modify the TPPS division A and B PLC programs to remove logic referencing the maintenance keys and maintenance mode.
  - b) Remove the maintenance key panel from TPPS rack PPS\_TGT: CAB01.
  - c) Remove the PLC input wiring associated with the maintenance mode key panel.

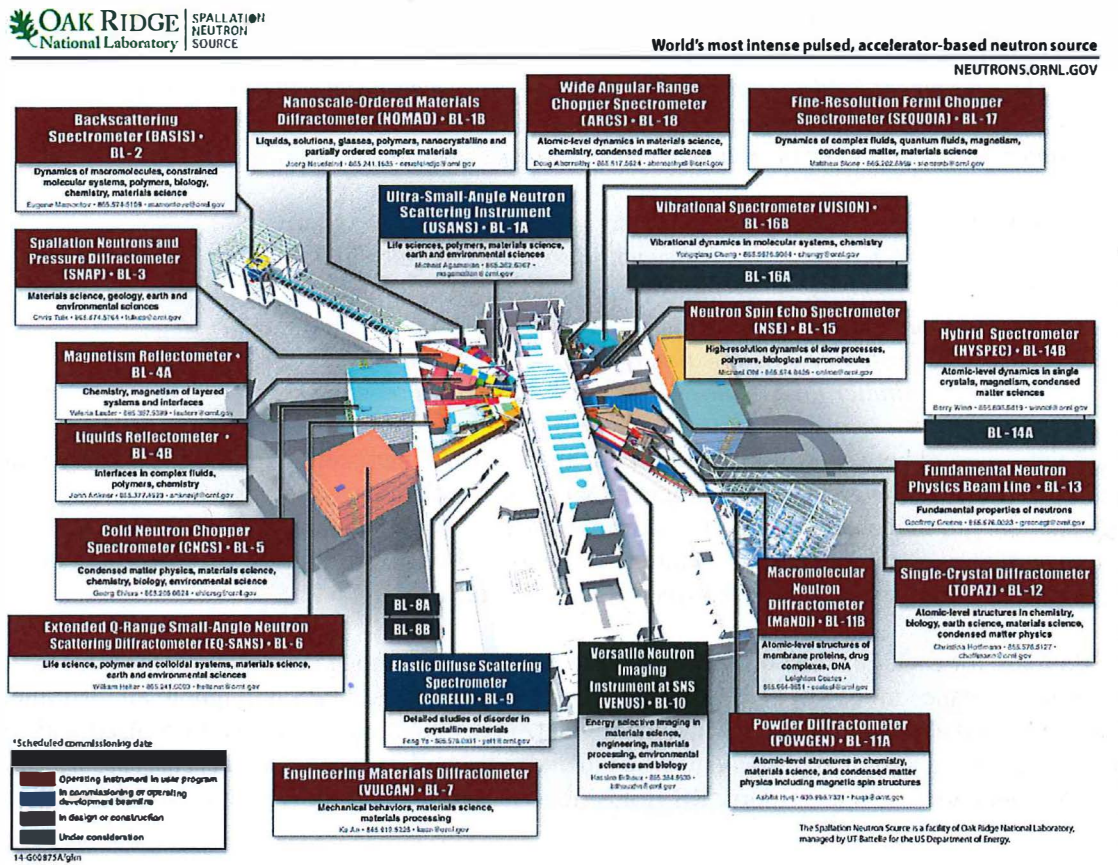


Figure 1 Maintenance Key Panel to be removed

## II.C Background

### II.C.1 Dual Beamlines

The SNS can supply neutron beam for up to 24 instruments through 18 beam ports arranged radially around the target monolith [see Figure 2]. Each of the 18 available beam ports is equipped with a Primary Shutter designed to stop the neutron beam at the monolith to allow safe access to an instrument enclosure. Closing the primary shutter for beamlines with two instruments, for example 11A and 11B, shuts off beam to both instruments. Some dual beamlines only have one of the two instruments in place with the second slot held for future expansion, e.g. 14A and 16A. Over the construction and commissioning of SNS, beam lines were added at a rate of approximately two per year. In 2014 SNS achieved its baseline of 16 operational beam ports and 19 instruments with the completion of instrument 1A (USANS).



**Figure 2** Target building instrument floor showing all SNS beamlines. Dual beamlines share a primary shutter and are designated by a letter (A/B) after the beamline number. The TPPS monitors status and fault signals from each beamline and relays the primary shutter OPEN/CLOSE commands sent from each instrument PPS. The TPPS can override an IPPS request to open a Primary Shutter if the partner beamline indicates an unsafe condition or an operator pushes an “Emergency Close” pushbutton.  
*Note: Beamlines 1A (USANS) and 9 (CORRELLI) are now operational.*

The original TPPS design includes internal wiring and PLC logic necessary to monitor all 24 instruments. The intent is that as beamlines are added, the IPPS is connected to the respective connections on the TPPS cabinets without having to re-program the TPPS. Currently, IPPS inputs from uninstalled instruments 8A, 8B, 10, 14A, and 16A are bypassed in the documented TPPS configuration. Special, configuration managed plugs at the TPPS are used to bypass the fault signals from these instruments. The plugs are fail-safe; if one is misconfigured the TPPS will register a fault condition and inhibit beam to the target.

## II.C.2 IPPS to TPPS Interface

Each instrument sends Access 1 OK, Access 2 OK and System Fault signals to the TPPS. The TPPS processes the Access and System faults based on a pre-determined logic and timing sequence. The timing sequence is based on the potential hazard for a given condition and is different for each beamline.

- a. If the instrument can resolve the fault before time 'x', it will reset the fault line to the TPPS and the TPPS will not take action.
- b. If the instrument cannot resolve the fault within time 'x', the TPPS will issue a Primary Shutter CLOSE command
- c. If the primary shutter does not close within time 'y', the TPPS will then perform the credited safety function to shut off the proton beam at the accelerator front end

This functionality is described in the FSAD-NF:

FSAD-NF 3.3.8.3.1.1 [TPPS] Overview:

*"If the instrument PPS cannot place the instrument in a safe state, the instrument PPS will provide a fault signal to the target PPS that will close the primary shutter or terminate the proton beam if necessary."*

FSAD-NF 5.2.17.2 [TPPS] System Description:

*"The target PPS monitors the instrument PPS status output (fault/no fault) for each of the instruments. When an instrument fault occurs, the target PPS trips the beam as needed to protect workers. For some instrument lines, the target PPS trips the proton beam immediately and for others it trips the proton beam if the primary shutter fails to close after a predetermined time interval."*

The total time allotted between an instrument fault and the TPPS performing the credited safety function is based on conservative worst case radiological exposure calculations assuming both secondary and primary shutters fail to close. The worst case accident exposure limit is provided by ORNL Radiological Protection and is presently limited to 500 mrem<sup>3</sup>. The total time before shutting off the proton beam varies for each instrument and ranges between 0 and 2 minutes.

The TPPS logic for each dual beamline includes the "maintenance mode key" input in the fault logic. When the maintenance mode keys are ON for a given instrument, the TPPS will ignore all instrument faults and inhibit the x and y timers for that instrument. This function is intended to be used with strict administrative configuration management which includes formally removing an instrument PPS from service and application of one or more 'RS Holds' to assure protection equivalent to the IPPS functions is in place.

The maintenance mode keys are under configuration management and locked in a special key box (See Figure 3). Access to the keys requires SNS operations management approval and a written work control plan.

In practice, the maintenance mode key switches have not been used and current staff are not familiar with their intended function and proper use. The Protection Systems Team engineering staff feel the key switches with the ability to bypass an instrument's fault lines within the TPPS PLC logic represents a vulnerability to errors in configuration management.

---

<sup>3</sup> SNS-OPM 02.H-4.1 Radiological Exposure-Administrative Limits section 5.2.



Figure 3 Maintenance Keys are under configuration management with an RS Hold lock.

## II.D Detailed Description of Changes:

Note: Engineering technical specification SNS-RAD-109090200-TS0001 gives a more detailed description of modifications described in this USI.

### II.D.1 Modify the primary shutter controls for beamlines 1A/1B and 11A/11B

- a. Remove the interim modification (relays K1, K2) for beamlines 1B and 11A and associated wiring
- b. Restore the BL 1B and 11A Access and System Fault wiring to the original terminal blocks
- c. Restore the BL 1 and 11 Primary Shutter OPEN command wiring to the original terminal blocks
- d. Modify the TPPS Division A software add conditions for BL 1 and BL 11 Primary Shutter OPEN command

#### Verification

- engineering design and documentation process
- checklists with “before/after” information
- independent verification that only intended changes were made
- use of before/after wiring documentation
- 100% verification of removals and additions using official documentation

### II.D.2 Remove the maintenance keyswitch panel and associated PLC program elements

- a. Remove the maintenance keyswitches and associated wiring from PPS\_TGT:CAB01.
- b. Disconnect field wiring from PPS\_TGT:CAB01 inside the TPPS cabinets PPS\_TGT:CAB05 and PPS\_TGT:CAB07.
- c. Modify the TPPS Division A and B PLC Logic to remove the program elements associated with the maintenance keyswitches and Maintenance Mode.

## Verification

- engineering design and documentation process
- creation of decommissioning drawing set
- checklists with “before/after” information
- independent verification that only intended changes were made
- use of before/after wiring documentation
- 100% verification of removals and additions using official documentation

## **II.E QA, Verification, and Validation**

In addition to design and change management processes for CECs defined in the SNS Operations Procedure Manual (OPM), the SNS Protection Systems Team utilizes lifecycle processes defined in ISO/IEC/IEEE 15288 “*Systems and software engineering — System life cycle processes*” to assure the final product meets the intended performance requirements.

Below is an outline of the processes used to assure the modifications described in this USI are correctly implemented.

### **II.E.1 Design Process:**

The design process ensures the intended modifications are evaluated and implemented through approved documentation.

- a. Protection system team leader (PSTL) approval of need for modifications and approval to proceed with the design
- b. Conceptual design review with protection system team (PST) engineering personnel
- c. Document changes detailed in Technical Specification SNS-RAD-109090200-TS0001
- d. Creation of de-installation drawings and revised as-built drawings
- e. PST engineer detailed PLC logic review and implementation by two engineers
- f. Independent PLC Logic review by competent engineer
- g. PLC A and B programs with these logic changes are part of the field integration testing being performed for the CCR racks.
- h. Target Personnel Protection System certification procedure SNS-OPM 3.A-7.4.12.H will be performed to validate maintenance key switch modifications.
- i. Post-maintenance test 1395587-PMT-000 will be performed to validate primary shutter operation.

The design basis for the hardware portion of the primary shutter control modification is based on accurate documentation generated at the time the relay modification was installed. The hardware design is essentially to go back to the original design without the relays. However, the drawing set for the TPPS cabinets is still advanced in revision level.

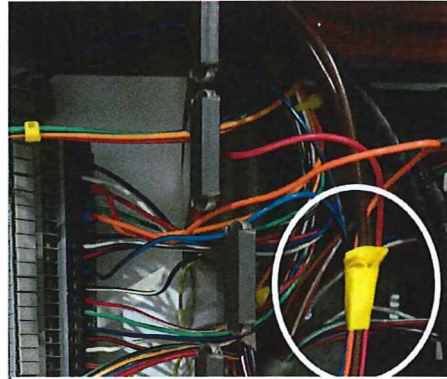
The design basis for the removal of the maintenance mode key switches is based on a 100% verification of the existing documentation. The systems engineer then created decommissioning drawings and prototype PLC logic modifications as the basis for the field modifications.

### **II.E.2 Implementation Process:**

#### Hardware Modifications

- II.E.2.1 Modification 1 Removal of the Primary Shutter OPEN inhibit relays and modification of PLC A logic shutter control

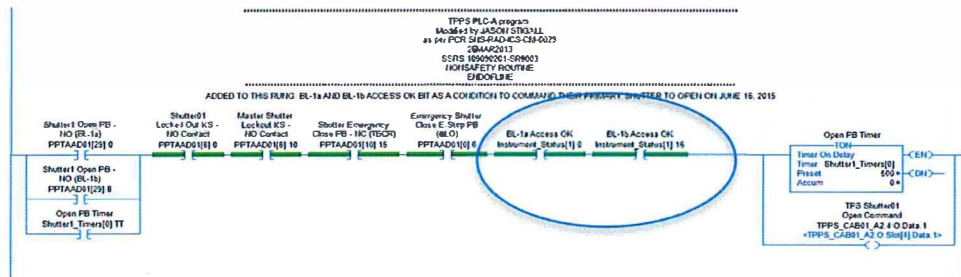
Hardware modifications include removing the relays and associated wiring installed in July 2014. The original installation was documented through configuration managed drawings. These drawings will guide the removal of the relays and wiring. The wiring associated with the relay installation is separated and marked to allow easy identification for removal (see Figure 4).



**Figure 4** Wiring for interim relay modification is marked for easy removal.

PLC program modifications will involve combining the Access faults and System fault bits into a single status bit, one for each of the individual dual beam lines, which indicates all faults for a respective beam line are in a safe state. This bit will be used to inhibit the primary shutter OPEN command if there is a fault on either of the two downstream beamlines.

*Note: The TPPS PLC A logic already contains this summary bit for each instrument beamline. The scope of the logic change will be to use the existing bits in the primary shutter OPEN logic string. Figure 5 is a representation of this addition.*



**Figure 5** Prototype TPPS PLC A logic showing the use of the BL-1A and BL-1B "Access OK" bit to inhibit the primary shutter OPEN command for beamline 1. The "Access OK" signal is a summary of all faults from a given instrument PPS.

II.E.2.2 Modification 2 Remove Maintenance Mode Key Switches and Logic

Hardware modifications involve removing the TPPS maintenance key switch panel and associated wiring from cabinet PPS\_TGT:CAB01. Because the revised drawings showing the wiring between TGT:CAB01 and the TPPS reflect the absence of key switches, the PPS Systems Engineer generated special

decommissioning drawings for each item to be removed. Figure 6 shows an example of the decommissioning drawing for the 1A/1B maintenance switches. These drawings are intended to guide the removal process only. The de-installation drawings are:

- DECOMMISSIONING DWG PPS\_TGT:CAB01 Target PPS LOCAL DEVICE WIRING BL-1A/B
- DECOMMISSIONING DWG PPS\_TGT:CAB01 Target PPS LOCAL DEVICE WIRING BL-4A/B
- DECOMMISSIONING DWG PPS\_TGT:CAB01 Target PPS LOCAL DEVICE WIRING BL-8A/B
- DECOMMISSIONING DWG PPS\_TGT:CAB01 Target PPS LOCAL DEVICE WIRING BL-11A/B
- DECOMMISSIONING DWG PPS\_TGT:CAB01 Target PPS LOCAL DEVICE WIRING BL-14A/B
- DECOMMISSIONING DWG PPS\_TGT:CAB01 Target PPS LOCAL DEVICE WIRING BL-16A/B

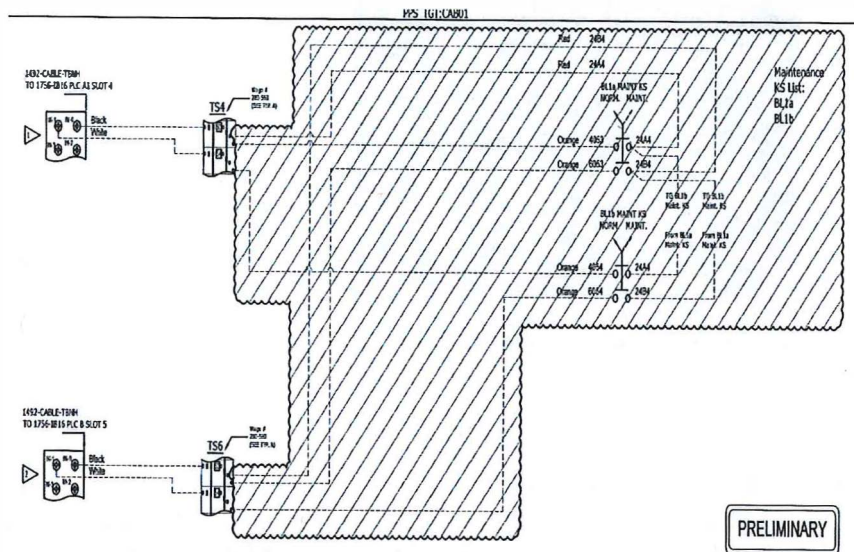


Figure 6 Typical decommissioning drawing used to remove the maintenance mode key panel and associated wiring.

The scope of software modifications is limited to removing all instances of the ‘maintenance mode’ within the TPPS PLC A and PLC B logic. Figure 7 shows a typical instance of the Maintenance Mode for beamline 1A that will be removed from the TPPS logic. There are no software modifications that affect the TPPS functionality or credited safety functions described in the FSADs.

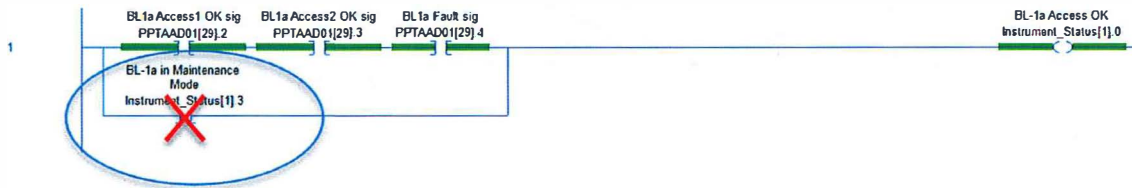


Figure 7 TPPS logic showing the "Maintenance Mode" bit that will be eliminated from the TPPS logic.

SNS-RAD-ICS-QA-0001 addresses the ten SQA criteria under the ORNL SQA SBMS subject area and DOE-O-414.1D and associated guidance 414.1-4A. SNS-RAD-ICS-PR-0014, “Software for Credited Engineering Controls”, is used to develop and implement PPS PLC modifications. Modifications for each PPS division (A/B) are performed by separate individuals. Engineering personnel performing the software modifications have training and experience in programming the PLC models used in both the existing and new TPPS.



The PLC software modification process included the following:

- Creation of before/after checklists for modified I/O
- Review of intended changes
- Modification of copies of the baseline PLC programs
- Simulated operation of the interface between the TPPS and each dual beamline
- Verification that only the intended changes were made using inspection and the PLC logic compare utility

### II.E.2.3 Integration Process

SNS personnel performed hardware and software integration testing during the laboratory test phase of the CCR rack modification project. The tests culminated in the successful completion of the formal integration test

SNS-RAD-ICS-PR-0036 R00 *“APPS Offline Integration Test for new PPS racks in CCR”*

Final integration testing will occur with the in-situ system after installation. The final integration tests include testing the TPPS with actual IPPS inputs where available before commissioning and certification. A post maintenance test procedure separate from the PPS CCR Rack Upgrade test procedure will be used to verify the modifications described in this USID and supporting engineering documentation are correct.

### II.E.2.4 Operations Documentation and Training

No operations related documentation or training is affected by this change.

## II.E.3 Testing and Verification Process:

### II.E.3.1 Laboratory Testing

PLC logic including modifications 1 and 2 were tested during the laboratory tests of the PPS CCR Rack Upgrade project. The TPPS PLC logic was first tested with only the modifications of re-mapped I/O as described in USID 102030102-ES0080. This formed the baseline logic configuration. Modifications 1 and 2 were then applied to the baseline and the system tested as a whole.

### II.E.3.2 Installation Testing

Installation will commence in late June 2015 during the SNS 2015 summer outage. During the installation period the TPPS systems will be formally removed from service.

The installed system will undergo five phases of testing:

1. Initial testing involves verifying basic functionality of the installed system with the modified PLC logic. Note that the hardware modifications are not absolutely required to effect the PLC program modifications. However, it is bad practice to leave non-functional hardware in a safety system.
2. Commissioning involves informal then formal verification all of the hardware modifications to the TPPS are implemented correctly. The commissioning of the modified TPPS will be performed as part of the commissioning process for the CCR PPS Rack Upgrade project. The results of commissioning will be recorded in SNS-RAD-ICS-PR-0038 *“APPS Commissioning Test for new PPS racks in CCR – complete system.”*
3. Post Maintenance Test (SNS-RAD-1395587-PMT-000) of the modified TPPS logic for PLCs A and B to verify the modified logic functions correctly and no unintended modifications were introduced into the system. This test includes a 100% verification of primary shutter controls for the dual beamlines.
4. Once commissioning is complete, the TPPS will undergo a full certification process along with the rest of the accelerator PPS. TPPS Certification procedures are under the SNS OPM section 3.A-7.4.12H and 3.A-7.4.12I.
5. In addition to performing the certification procedure for the TPPS, section A.3.8 of the SNS-

OPM 3.A-7.5.1A certification procedure for beam line 1A and section A.4.15 of the SNS-OPM 3.A-7.5.11B certification procedure for beam line 11B will be performed as validation of the proper functional response by the TPPS, under the condition when secondary shutter fails and one of these beam line has an Access or System fault.

At a minimum, SNS QA personnel will observe the initial inspection and certification testing. SNS QA, management, and DOE Site Office personnel may also perform random assessments at any stage of the process.

#### **II.F Conclusion of Section II**

The material presented in section II supports a negative USI determination as documented through the negative answers to the guiding questions in parts III and IV. Nor are there new failure modes or potential accidents introduced through this change. Rather, the changes described in this document improve the overall safety reliability of the installed TPPS system.

**III Does the proposed activity or discovered condition affect information presented in the FSAD-NF or FSAD-PF, e.g. regarding equipment, administrative controls, or safety analyses.**

If so specify the applicable FSAD and relevant sections.

No. The FSAD-PF and FSAD-NF does not address details to the level of the primary shutter control logic nor the dual shutter maintenance mode/maintenance keys. No changes to either FSAD will be needed as a result of the proposed modifications associated with the primary shutter operation or the removal of the maintenance mode.

**IV Does the proposed activity or discovered condition affect any of the requirements of the ASE.**

If so, list the affected sections

No. The PPS is specifically addressed in Section 3.2 of the ASE, *Personnel Protection System (PPS) and PPS-interlocked Area Radiation Monitor*. The ASE does not address details to the level of the primary shutter control logic nor the dual shutter maintenance mode/maintenance keys. The ASE is unaffected by the proposed modifications associated with the primary shutter operation or the removal of the maintenance mode.

**V USI Evaluation Criteria:**

1. Could the change significantly increase the probability of occurrence of an accident previously evaluated in the FSADs? Yes  No

**Justification:**

No. The probability of occurrence of an accident associated with accelerator produced prompt radiation is not affected by the proposed modifications associated with the primary shutter controls nor the removal of the maintenance mode. The proposed modifications do not affect the safety functionality of the PPS described in the FSADs.

2. Could the change significantly increase the consequences of an accident previously evaluated in the FSADs? Yes  No

**Justification:**

No. The PPS is a Credited Engineered Control credited with protecting workers from potentially injurious prompt radiation produced by accelerator operations. The consequences of accidents addressed in the FSADs (i.e. excessive prompt radiation exposure) are not affected by the proposed modifications associated with the primary shutter operation nor the removal of the maintenance mode.

3. Could the change significantly increase the probability of occurrence of a malfunction of equipment important to safety previously evaluated in the FSADs?

Yes  No

**Justification:**

No. By simplifying the operation of the TPPS with respect to dual beamline configurations, the probability of a PPS malfunction is actually decreased. The proposed modifications do not affect the safety functionality of the PPS described in the FSADs. Post maintenance testing/certification (see Section II.E.3 above) ensures proper system functionality following implementation of modifications.

4. Could the change significantly increase the consequences of a malfunction of equipment important to safety previously evaluated in the FSADs?

Yes\_\_ No

**Justification:**

No. The PPS is a Credited Engineered Control (CEC) credited with protecting workers from potentially injurious prompt radiation produced by accelerator operations. The potential safety consequences of a failure of the PPS system (i.e. excessive prompt radiation exposure) are grave and are unchanged by system modifications. The proposed modifications do not affect the safety functionality of the PPS described in the FSADs.

5. Could the change create the possibility of a different type of accident than any previously evaluated in the FSADs that would have potentially significant safety consequences?

Yes\_\_ No

**Justification:**

No. The proposed modifications do not increase the possibility of a different type of accident than those evaluated in the authorization basis that would have potentially significant safety consequences. The type of significant potential accidents associated with the TPPS system continues to be excessive personnel exposure to accelerator produced prompt radiation; no new types of accidents are created. The proposed modifications do not affect the safety functionality of the TPPS.

6. Could the change increase the possibility of a different type of malfunction of equipment important to safety than any previously evaluated in the FSADs?

Yes\_\_ No

**Justification:**


No. The proposed modifications will not increase the possibility of a different type of malfunction of equipment important to safety as evaluated in the FSADs. The proposed modifications do not affect the safety functionality of the PPS described in the FSADs. By simplifying the operation of the TPPS with respect to dual beamline configurations, the probability of a different type of malfunction is actually decreased. Post maintenance testing/certification (see Section II.E.3 above) verifies no new types of malfunctions have been introduced.


**VI. USI Determination:** A USI is determined to exist if the answer to any of the 6 questions above (Section V) is "Yes." If the answer to all 6 questions is "No", then no USI exists.

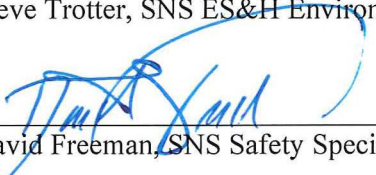
a. Does the proposed activity (or discovered condition) constitute a USI?


Yes – DOE approval required prior to implementing

No – Proposed activity may be implemented with appropriate internal review.

  
\_\_\_\_\_  
Kelly Mahoney, Protection Systems Team Leader, Qualified Preparer      14 July, 2015  
Date

  
\_\_\_\_\_  
Steve Trotter, SNS ES&H Environ. Waste Mngt., Qualified Reviewer      7-14-2015  
Date

  
\_\_\_\_\_  
David Freeman, SNS Safety Specialist, Qualified Reviewer      7/14/2015  
Date

  
\_\_\_\_\_  
Glen Johns, Accelerator Operations Group Leader, Reviewer      7-14-15  
Date

  
\_\_\_\_\_  
Hans Vogel, NSCD Directorate Operations Office Manager      7/16/15  
Date

**Approval:**

  
\_\_\_\_\_  
SNS Operations Manager of Designee      July 16, 2015  
Date

