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

I. Title of USI Evaluation: **BL11 and BL 1 PPS Logic Modification for Primary Shutter Control**

II. Description of Proposed Activity (or discovered condition) (use attachments if necessary):

It is proposed to add a relay logic circuit to the BL 11 and BL 1 Primary Shutter control logic to ensure that the Primary Shutter cannot be moved from the closed position when fault conditions are present.

Background

A weakness within the Personnel Protection System (PPS) control logic for the BL 11 Primary Shutter has been identified. The control logic weakness could allow the Primary Shutter to be temporarily moved out of the closed position following an Instrument Personnel Protection System (IPPS) forced closure initiated by fault conditions detected in BL 11B. It is proposed to modify the Primary Shutter control logic by the addition of hardware relay logic to prevent sending an open command to the Primary Shutter when fault conditions are present in the BL 11B IPPS control logic. This evaluation assesses 1) the proposed modification to correct the control logic weakness and 2) the potential radiological consequences associated with the existing configuration.

BL-11A and 11B share Primary Shutter 11. There is a single user panel from which a button is depressed to issue an open shutter command. Both beamlines are equipped with an IPPS controlled Secondary Shutter designed to independently prevent beam to the instrument. Normally, the Primary Shutter is opened for most of a run cycle and each instrument (BL 11A and BL 11B) utilizes its Secondary Shutter to prevent beam and to allow access into the instrument enclosures.

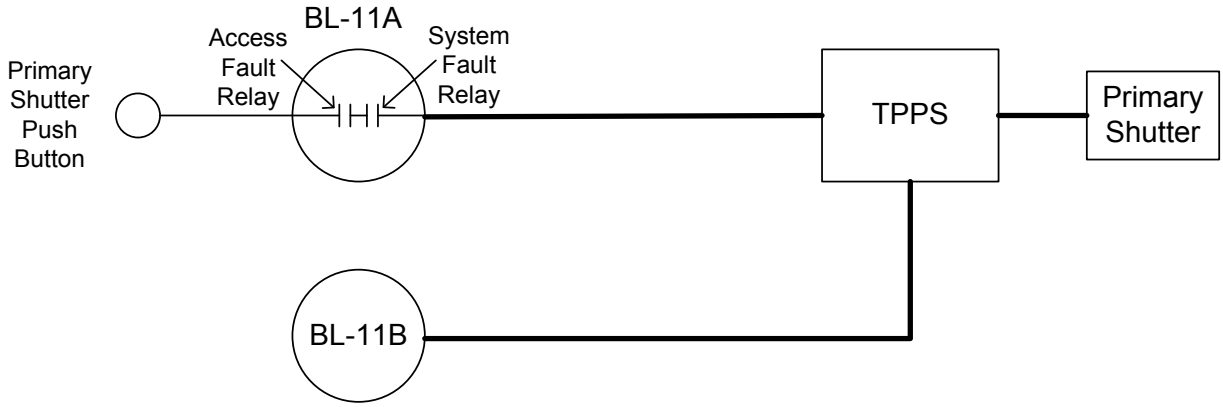
The IPPS system control logic for BL 11B, as described in the SSRS[1], issues commands to terminate beam to instrument enclosures if a *fault* condition occurs during beam operations. Fault conditions include *access faults* (e.g. opening of enclosure door with beam on) and *system faults* (e.g. PLC Input/Output module failure).

When a fault occurs during beam operations, the IPPS maintains the fault status output until the Secondary Shutter reaches the closed position. If the Secondary Shutter fails to reach the closed position within 30 seconds from issuance of the close command, the Target Personnel Protection System (TPPS), which controls movement of the Primary Shutter, commands the Primary Shutter to close. If the Primary Shutter fails to reach its closed position with 90 seconds of issuance of the close command (120 seconds after the fault was initially generated), the final reach-back sequence is extended to the Front-End systems and proton beam production is instantly terminated.

1 *IPPS Software Safety Requirements Specification MANDI (BL11b)*, SNS 109090200-SR0018-R00, November 3, 2011.

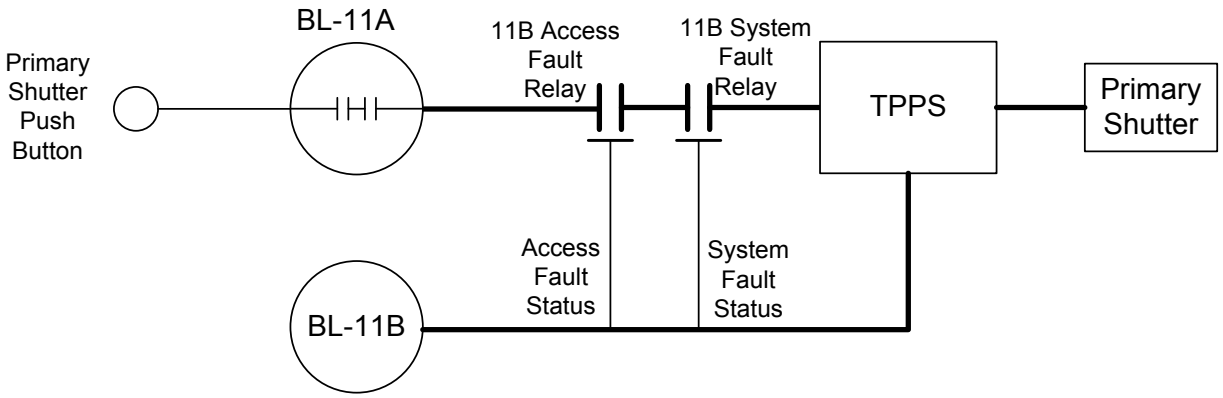
It is intended for the control logic to prevent the Primary Shutter from opening if access or system fault conditions exist. IPPS control logic for BL 11A includes access faults and system faults in the PLC logic chain of required conditions that must be met in order to issue an open shutter command to the Primary Shutter when the control button is depressed. The weakness identified in the BL 11B control logic is that the access faults and system fault are not part of the logic chain of required events to be satisfied in order to open the Primary Shutter. This weakness allows for the possibility that an open command could be issued and transmitted to the Primary Shutter by depressing the control panel button when a fault condition persists within the BL 11B control logic.

The present configuration is depicted in the figure below that shows the Access Fault and System Faults depicted as relays (note: although depicted in the figure as relays, the BL 11A logic is implemented with PLC logic, not physical relays) within the BL-11A control logic where none exists within the BL 11B control logic. The Primary Shutter "open" push button is located in the BL 11-A logic chain that can be thought of as the *Master* signal chain. The BL-11B signal is provided to the Target Personnel Protection System (TPPS) logic that requires a safe (high) signal from both BL 11A and 11B. As can be seen in the diagram below, either an Access Fault or a System Fault within BL 11A prevents the push button open command from reaching the TPPS. However, in the current configuration, BL 11B Access and System Faults are not incorporated in the open command logic. Faults from both beam lines are included in the TPPS close command logic. However, when the Primary Shutter reaches the closed position due to an access or system fault, the close command goes away.



Proposed Modification to Correct Logic Weakness

The proposed modification is to add relay logic with physical hardware relays to interrupt an open shutter command should Access or System Faults exist on BL 11B. The proposed modification is depicted in the figure below. Two physical hardware relays will be installed in the BL-11A master command chain for opening of the Primary Shutter. If either an Access or System Fault exists in BL 11B, the respective relay will create an "open circuit condition" effectively preventing the open request from reaching the TPPS.



The relays will be physically located in the TPPS-Cab07 control cabinet as shown on modified drawings 109090201-R8U-8700-A117, Rev1 and 109090201-R8U-8700-A105, Rev1. The relays will add the fault statuses from BL-11B to the Primary shutter "Open" request signal that is generated at BL-11A and sent to TPPS.

A parallel condition has been identified during the initial certification process for newly installed (but not operational) BL 1A. The same logic configuration weakness was found with the newly installed (but yet to be certified) BL-1A IPPS with the difference being that BL 1B serves as the *Master* controller and BL-1A serves as the *Slave* controller. The evaluation presented here is equally valid for BL 1 shutter control logic. The same hardware logic modification described above for BL-11 will be will be implemented for the BL-1 Primary Shutter control. Two relays will be physically located in the TPPS-Cab05 control cabinet as shown on modified drawings 109090201-R8U-8700-A083, Rev1 and 109090201-R8U-8700-A071, Rev1.

Once approved, the proposed modification will be implemented in accordance with approved written procedures. Appropriate post maintenance testing will be conducted prior to operations in accordance with approved written procedures to ensure system functionality.

Potential Radiological Consequences – Inadvertent Opening of Shutter

The existing logic creates the potential for an open signal to be transmitted to the BL 11 Primary Shutter in the presence of a fault condition (e.g. potential to transport beam into an unsecured beam enclosure). In such an instance, the Primary Shutter would begin to move out of the closed position towards the open position. Once the Primary Shutter were to lift off of the shutter closed position indicators, the IPPS shutter timers would be reset and begin counting from t = 0. If a fault condition existed with the potential for beam into an accessible enclosure, the IPPS control logic would send a close shutter command to Secondary Shutter at t = 0. If the Secondary Shutter does not close within 30 seconds, the Primary Shutter close sequence would be initiated. If the Primary Shutter does not close within 90 seconds of the close command, proton beam production would be terminated.

A worst-case accident condition would be personnel access into the enclosure with the Secondary Shutter open and Primary Shutter not closed. Assuming such a fault were to occur, the IPPS would effectively terminate the hazard as described above; however, because of the logic weakness, it would be possible to move the Primary Shutter out of the fully closed position

with the Secondary Shutter failed in the open position. In such an instance, the Primary Shutter would drive towards the open position for 30 seconds before receiving a close command that would reverse the shutter direction and drive the shutter closed.

Recently measured travel times for the BL 11 Primary Shutter showed 44 seconds from fully closed to fully opened, and 68 seconds from fully opened to fully closed.[2] The Primary Shutter has a stroke (distance of travel) of 20 inches from fully open to fully closed. Examination of dimensions provided in the Primary Shutter, Shutter Insert and Core Vessel Insert drawings conservatively indicate that the shutter must move 10.5 inches from the fully closed position before line of sight streaming through the Shutter Insert could occur[3]. If we assume constant travel speed, we can calculate the time required from the issuance of the open command before streaming could start to occur as follows:

$$\frac{44\ seconds\ to\ open}{20\ inch\ travel} \cdot 10.5\ inch\ travel = 23.1\ seconds$$

We can also calculate how far the shutter drives open within the 30-second time frame before the IPPS command to close is issued:

$$\frac{20\ inch\ travel}{44\ seconds\ to\ open} \cdot 30\ seconds = 13.6\ inches\ from\ the\ closed\ position$$

Therefore, we see that the Primary Shutter would not fully open, however, it could begin to partially open at 23.1 seconds allowing a streaming path as the shutter moved from 10.5 to 13.6 inches from the closed position over the time frame of 30 - 23.1 = 6.9 seconds.

At 13.6 inches (t = 30 seconds) of travel, the shutter would reverse direction and drive closed. We can calculate the time to close the streaming path based on the measured time to close as follows:

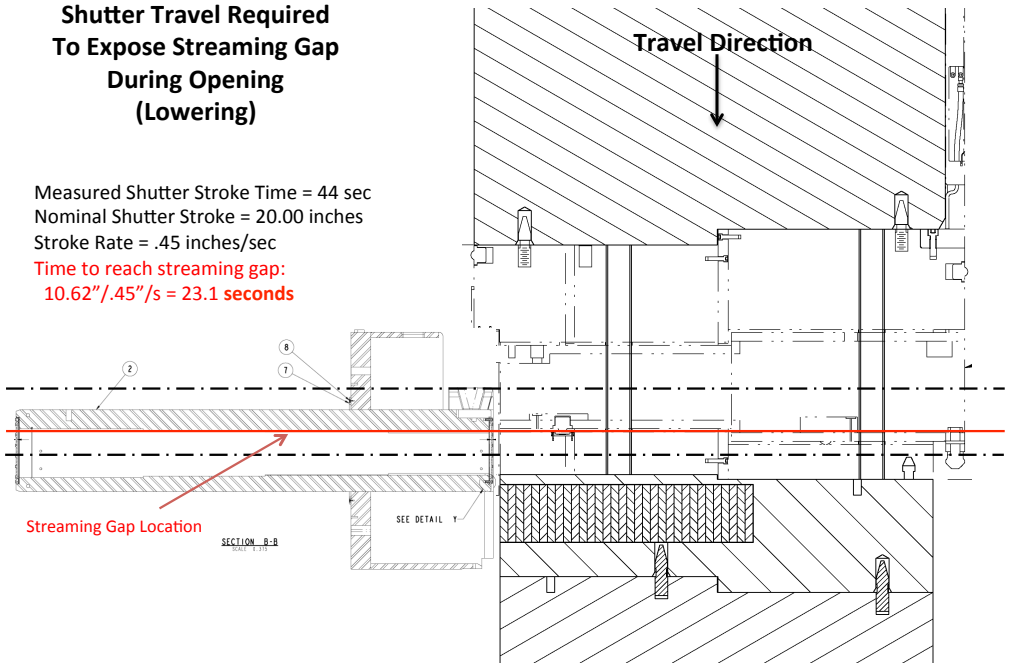
$$\frac{68\ seconds\ to\ close}{20\ inch\ travel} \cdot (13.6\ inch - 10.5\ inch) = 10.5\ seconds$$

Based on the above assumptions, we could estimate open streaming path could be open for 6.9 + 10.5 = 17.4 seconds.

2 *Shutter Cycle Times*, Email form D. Curry to D. Freeman, June 4, 2014.
3 *BL 11 Shutter Dimensions*, Email from M. Dayton to D. Freeman, June 4, 2014.

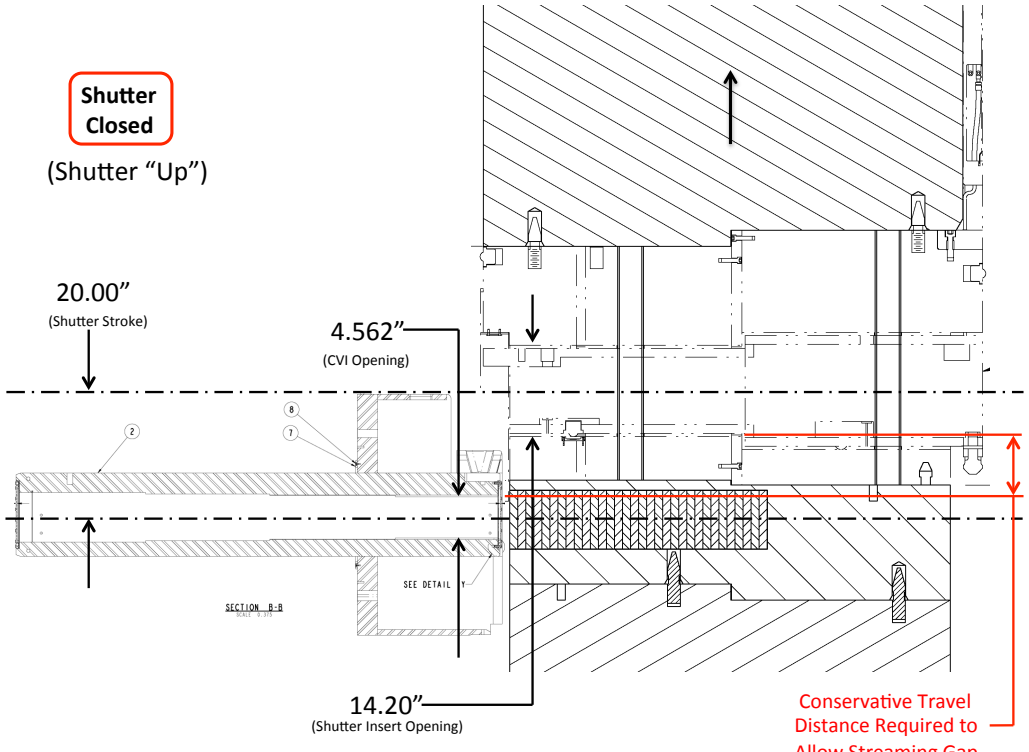
Shutter Travel Required To Expose Streaming Gap During Opening (Lowering)

Measured Shutter Stroke Time = 44 sec
Nominal Shutter Stroke = 20.00 inches
Stroke Rate = .45 inches/sec
Time to reach streaming gap:
10.62”/.45”/s = 23.1 **seconds**



Shutter Closed

(Shutter “Up”)



$$Travel = 20.00 - 14.20/2 - 4.562/2 = 10.62 \; inches$$

The maximum in-beam dose rate for BL 11B at 1.4 MW has been calculated to be 7 R/hr.[4] It is highly unlikely that an individual would be in the direct beam because the beamline components would have to be disassembled to access direct beam and the beam is readily accessible. If an individual were to access the streaming beam during such an unlikely scenario, the size of the partially open beam is small such that any exposure would be highly localized rather than a whole body dose exposure. If we assume a weighting factor of 0.5 to account for differences in whole body exposure to localized beam exposure, we could estimate the worst case dose to an individual exposed while the Primary Shutter cycled for open to closed as follows:

$$\frac{7R}{hr} \cdot \frac{1hr}{3600\ sec} \cdot 17.4\,\text{sec}\ exposure \cdot 0.5\ weighing\ factor = 17\ millirem$$

One could further assume that an individual could repeatedly attempt to reopen the shutter even thought the shutter would automatically drive back in each time. Assuming an individual attempted to reopen the shutter 3 times before finally seeking assistance, an associated worst-case accident dose could be as high as (3 x 17 mrem) 51 mrem. The accident dose of 51 mrem is well below the 5 Rem statutory annual dose limit established in 10 CFR 835 and even significantly below the ORNL ALARA goal of 600 mrem/yr established for routine (non-accident) dose to workers. Therefore it is concluded that the potential to receive a significant dose is not possible.

The above scenario assumes an individual stands in the direct beam path during a postulated scenario where another individual attempts to repeatedly open the Primary Shutter following IPPS forced closure initiated from a Secondary Shutter closed fault condition. If the individual is assumed to be within the instrument enclosure, a much more likely scenario would be that the individual would be standing near the beam path rather than in the direct beam because the beam line is normally not disassembled. The worst-case dose rate during instrument operations is 20 mrem/hr at a distance of 30 cm assuming the beam strikes a large steel sample[4]. Under this much more likely assumption, the dose to an individual during inadvertent cycling of the Primary Shutter can be estimated as follows:

$$\frac{20\ mrem}{hr} \cdot \frac{1hr}{3600\ sec} \cdot 17.4\,\text{sec}\ exposure \cdot 1.0\ weighing\ factor = 1\ mrem$$

Assuming as above, that an individual attempts to repeatedly open the Primary Shutter three times after the IPPS forced closure of the shutter, the individual in the instrument enclosure could receive up to 3 mrem.

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-NF and FSAD-PF describe the IPPS system but do not address detailed logic architecture that would be affected by the proposed changes.

4 Popova, I, *Shielding for MANDI Instrument Enclosure*, SNS-106100200-DA0053-R00, April 2012.

IV. Does the proposed activity or discovered condition affect any of the requirements of the ASE. If so, list the affected sections

No, the ASE does not address specifics regarding IPPS control logic architecture and is not affected by the proposed changes.

V. USI Evaluation Criteria:

1. Could the change significantly increase the probability of occurrence of an accident previously evaluated in the FSADs? Yes __ No_x_

   Justification: No, the proposed modification will improve the Shutter Open command control logic to prevent movement in the presence of Access or System Faults. The proposed modification has no affect on the probability of occurrence of any accident evaluated in the FSADs. The potential radiological consequence associated with the present configuration is not safety significant as shown by the analysis presented above.

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

   Justification: No, the proposed modification will improve the Shutter Open command control logic to prevent movement in the presence of Access or System Faults. The proposed modification has no affect on the consequences of any accident evaluated in the FSADs. The potential radiological consequence associated with the present configuration is not safety significant as shown by the analysis presented above.

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 _x_

   Justification: No, the proposed modification will improve the Shutter Open command control logic to prevent movement in the presence of Access or System Faults. The proposed modification will not increase the probability of a malfunction of the PPS or Primary Shutter or any other safety equipment evaluated in the FSADs. The potential radiological consequence associated with the present configuration is not safety significant as shown by the analysis presented above.

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

   Yes__ No _x_

   Justification: No, the proposed modification will improve the Shutter Open command control logic to prevent movement in the presence of Access or System Faults. Consequences of malfunction of equipment important to safety as evaluated in the FSADs are not affected by the proposed modification. The proposed modification will not increase consequences of a malfunction of the PPS or Primary Shutter or any other safety equipment evaluated in the FSADs. The potential radiological consequence associated with the present configuration is not safety significant as shown by the analysis presented above.

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 _x_

   Justification: No, the proposed modification will improve the Shutter Open command control logic to prevent movement in the presence of Access or System Faults. The proposed modification will not create the possibility of a different type of accident with potentially significant safety consequences. The proposed modification will undergo peer review and review by the SNS Configuration Control Committee. Additionally, use of approved procedures to implement the modification and to conduct post modification testing will add assurance of proper system functionality.

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 _x_

   Justification: No, the proposed modification will improve the Shutter Open command control logic to prevent movement in the presence of Access or System Faults. The proposed modification will not create the possibility of a different type of equipment malfunction important to safety. The proposed modification will undergo peer review and review by the SNS Configuration Control Committee. Additionally, use of approved procedures to implement the modification and to conduct post modification testing will add assurance of proper system functionality.

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

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

David Freeman, SNS Safety Specialist, Qualified Preparer — Date: 6/9/2014

Mike Harrington, Qualified Reviewer — Date: 6/9/2014

Kelley Mahoney, PST Team Leader — Date: 6/9/2014

Don Gregory, SNS Radiation Safety Officer — Date: 9 JUNE 2014

Bobby Cross, SNS Instrument Operations Manager — Date: 6/9/2014

Approvals:

Signature of SNS Operations Manager or Designee — Date: June 09, 2014