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

I. Title of USI Evaluation:

USI Evaluation for the PPS Redundant 24 Volt Power Supply Failure

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

This USI Evaluation assesses the discovered condition of a malfunction of the PPS during a routine annual certification. It was discovered that certain safety functions of the PPS were inoperable because of a common mode failure of the HEBT segment Input/Output modules.

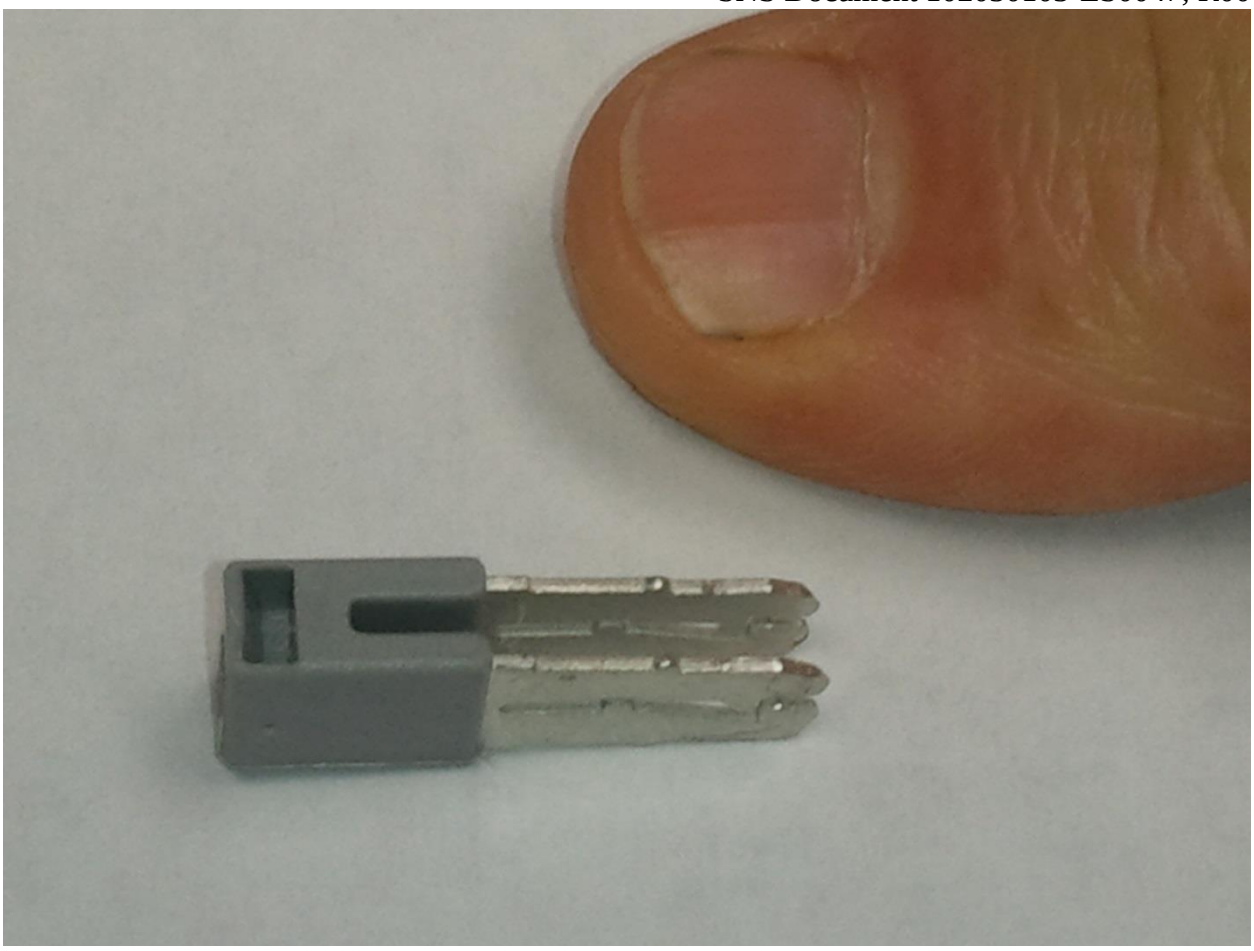
Background

The PPS, as described in the Spallation Neutron Source Final Safety Assessment Document for Proton Facilities SNS102030103-ES0018-R02, December 2010 (FSAD-PF) is a Credited Engineered Control (CEC) the primary function of which is to protect workers from potentially injurious prompt radiation produced by accelerator operations. The PPS is responsible for the following credited safety functions as listed in the FSAD-PF, section 5.2.1.1

- Prevent beam operation in segments not cleared of personnel (beam containment).
- Shut off beam if personnel enter an operating segment.
- Shut off beam if the Target carriage is not in position to receive beam.
- Shut off beam if equipment faults or other failures cause radiation levels to increase over acceptable levels in occupied areas.

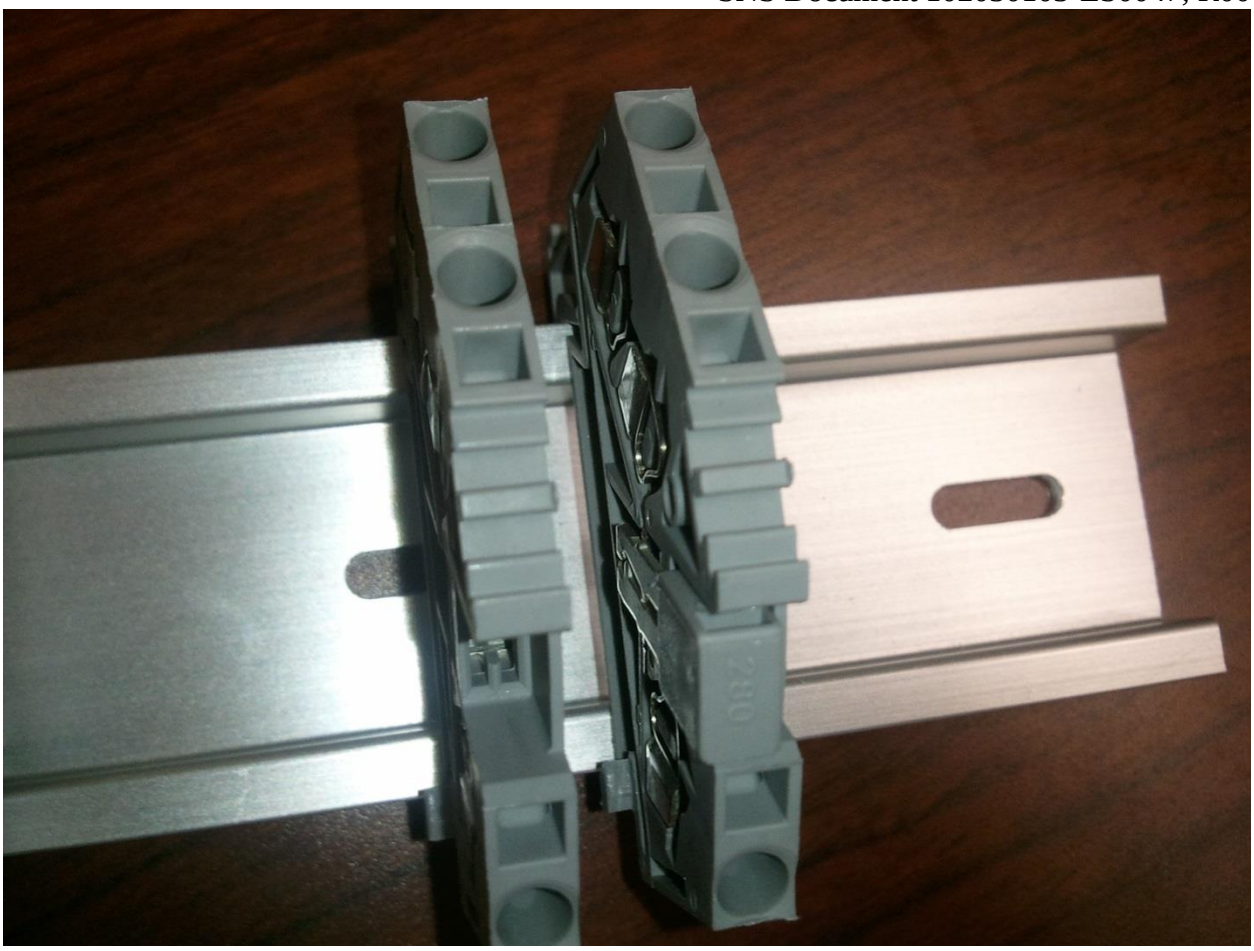
During a required neutron beamline IPPS certification procedure performed as part of the 2013 summer maintenance outage, it was discovered that the PPS was malfunctioning. Subsequent investigations discovered that the malfunction was caused by an improperly installed jumper and design weaknesses that rendered the system incapable of performing certain required safety functions. The improperly installed jumper connector was intended to provide continuity between common and ground DIN rail modules. Although the jumper visually appeared to be in its required position, it was not properly seated and therefore was not providing continuity between the common and ground busses as required. Post maintenance testing was performed, but was not adequate to identify the lack of continuity between ground and common terminals caused by the incorrectly installed jumper.

The term “jumper” refers to a 2-pronged commercially available circuit building element used with rail mounted terminal blocks. A typical jumper and terminal blocks are shown in Photographs 1 and 2 below.

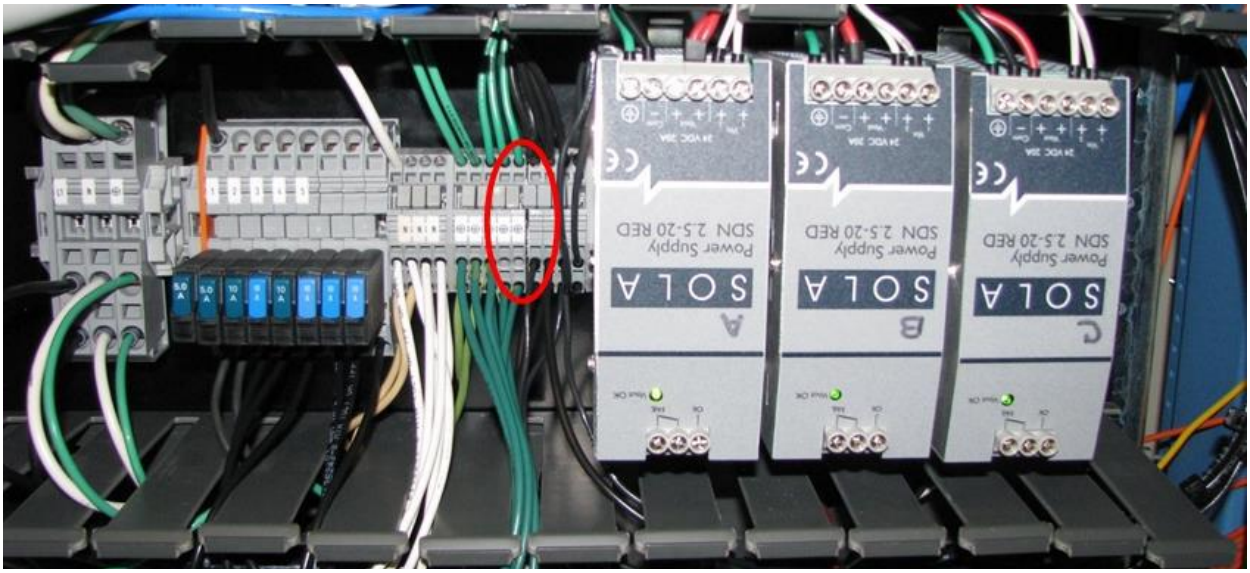


Photograph 1. Typical jumper

The installation failure referred to above occurred when the jumper was inserted between terminal blocks but failed to make electrical contact with the adjacent terminal block element. An exaggeration of such a condition is depicted in Photograph 2. Photograph 3 shows the actual as found improperly installed jumper that lead to the system failure. The photograph shows a gap between the adjacent terminal blocks. The improper installation allowed the "common" input of each channel to float instead of being grounded.



Photograph 2. Exaggeration of Improperly installed Jumper. Note the jumper cannot bridge the gap between the two DIN modules.



Photograph 3. Actual Photograph of Improperly Installed Jumper Causing PPS Failure. (Note the improperly installed jumper circled in red.)

Investigations of the system design identified weaknesses that 1) created the potential for a common mode failure between the normally independent A and B channels and 2) made the circuit susceptible to unsafe failure in the absence of correct jumper installation. The common mode failure design weakness was created in April 2013 when redundant power supplies were installed in channel A and channel B in an effort to increase system reliability. The redundant power supplies were installed under an approved CEC Permanent Change Request 109090101-CM0022-R01. Figure 1 presents a schematic depiction of the system with the redundant power supplies in place. As shown in the figure, the common legs and ground legs of both 24 VDC Redundant HEBT A and B modules are tied to a common buss and the common and ground portions of the buss are isolated by the lack of jumper contact.

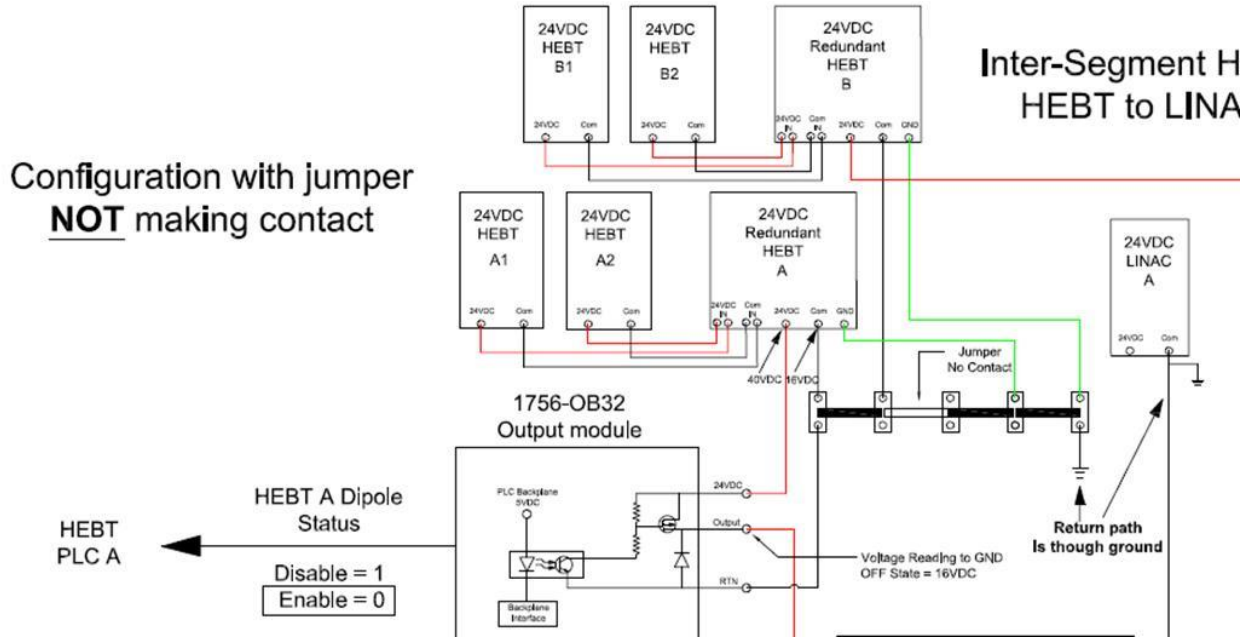


Figure 1. Schematic Depiction of PPS Redundant Power Supply Circuit

Prior to the installation of the redundant power supplies, Channel A and B were independent and not susceptible to common mode failure. Had the installation design maintained channel independence, an improperly installed jumper on a particular channel would have made that channel susceptible to an unsafe failure; however the other channel would have been unaffected. The probability of improper jumper placement in two independent channels would have been highly unlikely.

The redundant power supply installed with the improperly installed jumper was installed on April 2 2013 as part of an initiative to replace single 24 Volt power supplies with redundant 24 Volt power supplies with the goal of improving system reliability. SNS operated at a power of ~ 850 kW throughout both April and May 2013. Because the ASE requires the PPS to be completely operational for beam operations; this event has been categorized as an ASE violation. The purpose of this USI Evaluation is to determine if the discovered condition also constitutes an Unreviewed Safety Issue.

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.

The PPS system and its architecture are described in both the FSAD-PF and FSAD-NF; however the level of detail regarding how individual power supplies are wired is not addressed. The System Architecture of the Personnel Protection System (PPS) is described in 3.2.3.4 of the FSAD-PF. Section 3.2.3.4.1 "PLC Hardware" states that: "*Each redundant PLC in a one-out-of-two configuration is maintained as a separate system to minimize common mode failures*". In the original implementation of the PPS, the A and B channel Input/Output modules were powered by separate, independent power supplies. The design was modified as described in a Permanent Change Request SNS-OPM-AT 3.A-8.1.a (Request 109090101-CM0022-R01) to include a second, redundant, power supply for each channel for the purpose of increased reliability. In the detailed field implementation, not described in the PCR, the two power supplies for each channel were fed into Redundancy Modules, one for the A channel and one for the B channel. Both Redundancy Modules were mounted on a shared DIN Rail with shared terminal blocks for the Redundancy Module common connections and a shared terminal block for the Redundancy Module grounds for the A channel and B channel connections to building ground. This common mounting and grounding configuration is not in accord with the description of the PPS system Architecture.

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

The discovered condition was that of impaired operability of the HEBT section of the PPS during a period of beam operations. This is considered to be a violation of ASE section 3.2.1.

The relevant section of the ASE, Section 3.2 states:

3.2 Personnel Protection System (PPS) and PPS-interlocked Area Radiation Monitor system:
The PPS and Area Radiation Monitors that are interlocked to the PPS 1) prevent entry In areas with significant radiation hazard 2) trip the beam off when radiation levels set by the SNS RSO are reached in occupied areas, and 3) prohibit beam to the target when the target cart is out of "cart-inserted" position. .

3.2.1 Operability - Those portions of the PPS and PPS-interlocked Area Radiation Monitor systems required to support the applicable operational configuration shall be operable during operations with beam.

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: The PPS is a Credited Engineered Control (CEC) whose primary function is to protect workers from potentially injurious prompt radiation produced by accelerator operations. The unmitigated probability of occurrence of an accident associated with the PPS

is not affected by the functionality of the PPS system. Although the ability of the PPS to perform its intended mitigative safety functions was impaired, the probability of occurrence of unmitigated accidents was unaffected.

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

   Justification: The PPS is a Credited Engineered Control (CEC) whose primary function is to protect workers from potentially injurious prompt radiation produced by accelerator operations. Although the ability of the PPS to perform its intended mitigative safety functions was impaired, the unmitigated consequences (i.e. potential radiation exposures due to an accident without PPS protective actions) are unaffected by the functionality of the PPS.

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

   Yes_x_ No __

   Justification: The PPS is a Credited Engineered Control (CEC) the primary function of which is to protect workers from potentially injurious prompt radiation produced by accelerator operations. The impaired nature of the HEBT segment of the PPS was a result of a common mode failure the probability of which was significantly increased by the installation of the redundant 24VDC power supply to the PPS. Weaknesses in the design and installation of the redundant power supplies increased the failure probability of the system by introducing a common mode failure into isolated channels. Improper installation of the jumper caused an unsafe failure of the system. Therefore the probability of occurrence of a malfunction of the PPS system was significantly increased.

   The analysis provided in Appendix A shows that the required SIL-2 reliability of the PPS system can be maintained with the current configuration of the redundant 24 Volt PPS power supplies by 1) verifying that all redundant power supplies are properly installed and operable, 2) minimizing access to the cabinets and enforcing strict configuration control and 3) by testing the system functionality at least once every 18 days. Testing the system functionality every 18 days maintains the probability of occurrence of a system failure on demand within the FSAD-PF specified SIL-2 values. With the above controls in place, the probability of occurrence of a malfunction due to the presence of the PPS 24 Volt redundant power supplies is not significantly increased beyond that assumed in the FSAD-PF.

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: The PPS is a Credited Engineered Control (CEC) the primary function of which is to protect workers from potentially injurious prompt radiation produced by accelerator operations. The consequences of a failure of the PPS system were unchanged by the PPS malfunction.

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: The impaired nature of the HEBT Segment of the PPS did not increase the possibility of a different type of accident than any previously evaluated in the authorization basis that would have potentially significant safety consequences. Although the ability of the PPS to perform its intended mitigative safety functions was impaired, no new types of accidents were created.

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: The FSADs evaluate accidents and determine the need for mitigative safety controls based on the potential consequences and probabilities of accidents. The PPS is required to mitigate/prevent unacceptable accident risks. It was recognized that PPS failures must be made to be very unlikely, so the dual independent channel architecture was adopted. It was recognized that even with two independent channels in a 1-of-2 structure, that common mode failures were possible, but were made highly unlikely by the channel separation. The compromise of channel separation leading to impairment of the PPS was not a new or unrecognized failure mode.

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?

_x_ Yes – DOE approval required

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

David Freeman, Qualified Preparer — 8/9/2013 — Date

Mike Harrington, Qualified Reviewer — 8/9/2013 — Date

Approvals:

George Dodson, Deputy Division Director — 8/9/2013 — Date

Kevin Jones, RAD Division Director — 08/09/2013 — Date

Crystal Schrof, NSCD Operations — 8-9-2013

Appendix A. Determination of Suitable Test Interval for PPS Redundant 24 Volt Power Supplies With Common Mode Failure Vulnerability

As described in Section 5.2 of the FSAD-PF, the PPS has followed established industry standards (e.g. ANSI/ISA-84.00.01, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*) to guide the safety life cycle from design, procurement, fabrication, testing, to operation and maintenance. Per this standard, the PPS safety functions have been evaluated and categorized as to safety integrity level. The most critical PPS safety functions are designed to meet or exceed safety integrity level 2 (SIL-2) per the standard. By definition, a SIL-2 rated system has a probability of success upon demand of greater than 0.99 (conversely, a SIL-2 rated system has probability of failure upon demand of less than 0.01).

SNS desires to operate on an interim basis with redundant power supplies installed that are vulnerable to a common mode failure of a break in the common to ground connection. All of the common to ground connections associated with installed redundant power supplies have been tested and verified to be in the proper configuration and to be functioning properly. Additionally, the cabinets have been locked and modificationscan only be accessed under strict configuration control. Therefore it highly unlikely that a common mode failure break between the common and ground connections of the redundant power supplies could spontaneously occur.

One could postulate that perhaps a wire or jumper could break either spontaneously or due to some sort of unanticipated and unidentified energetic event. Operating experience with the DIN racks has shown the wiring in the DIN racks to be very reliable and that they are not susceptible to spontaneous wire/jumper breaks. None-the-less one could postulate a conservative spontaneous mean time between failures (MTBF) probability of 10 years for a ground to common jumper/wire connection within the installed redundant power supplies. The assumption that a probability of 0.1/y is conservative for spontaneous failure on wire connections is based on 10 years of experience with the PPS.

The probability of failure can be related to the testing interval in accordance to the methodology presented in Target Protection System Failure Probability Analysis[1] which relates probability of failure on demand (POFD) to testing interval as follows:

$$POFD = \frac{1}{MTBF(yrs)} \cdot \frac{Test\ Interval\ (months)}{12\ months/yr}$$

As discussed above, SIL-2 allows for a POFD as large as 0.01. If we allocate half of that margin (POFD of 0.005) to all other random failures within the system, and allocate the other

1 Wayne Weaver, Nutherm Failure Probability Analysis for the Target Protection System Spallation Neutron Source, ONL-9029FA, Rev. 1, March 2006.

half (POFD of 0.005) to a spontaneous beak in the common to ground wire/jumper connection, then we can solve the above equation to obtain a suitable test interval as shown below.

$$Test\ Interval\ (months) = POFD \cdot MTBF(yrs) \cdot 12\ months/yr$$
$$= 0.005 \cdot 10yr \cdot 12months/yr = 0.6\ months = 18.3\ day$$

Therefore, an 18.3 day test interval would be sufficient to ensure that an assumed spontaneous break in the common to ground connection in one of the PPS redundant 24 Volt power supplies would be adequately protected against at the SIL-2 level.

The proposed routine weekly testing (interval not to exceed 18.3 days) would meet the SIL-2 reliability objective with a margin of safety.