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

I Title of USI Evaluation:

USI Evaluation for the Changes Associated with Replacement of CCR PPS Rack Cabinets 03, 04, 05, and 06.

II Description of Proposed Activity (or discovered condition):

This USI evaluation addresses the final modifications to eliminate the Central Control Room (CCR) PPS rack common mode ground vulnerability identified in July 2013[1]. The final modifications include replacing four CCR PPS racks CAB03-CAB06 with modified and fully tested replacement racks. The replacement racks contain the necessary wiring, hardware, and program modifications described in this evaluation and associated change documentation.
Interim modifications implemented in January 2014 greatly reduced, but did not eliminate the potential vulnerability[2]. The final modifications described in this USI and associated change documentation complete the action to eliminate the identified failure mode in the CCR PPS racks.
In order to ensure maximum time for test and QA, and to minimize SNS downtime, it is proposed to completely replace the four affected CCR PPS rack cabinets (03, 04, 05 and 06) with four modified and fully tested rack cabinets. The proposed modifications are to rack wiring methods and layout as well as replacing obsolescent components only. The system description and safety functions performed by the PPS systems under the current FSAD-PF, FSAD-NF and approved ASE remain unchanged.

II.A Summary of Changes to Hardware and Equipment

The new racks incorporate the following hardware changes and improvements when compared to the existing racks:

1. Isolated DC power returns between each PPS division (A/B) and from earth ground to eliminate the common mode vulnerability discovered in July 2013.
2. Replaced DC return shorting clips with a power distribution module. This eliminates the direct cause for creating an open return path discovered in July 2013.
3. Replaced the 30 redundant DC power supplies and 15 redundancy switchover units installed in April 2013 with 6 isolated DC power supplies. This greatly reduces the complexity and potential failure modes of the PPS with minimal impact to system availability.
4. Re-arrangement of certain PLC inputs/outputs to separate important signals like inter-segment status and less important signals like panel lamps. This modification improves the reliability of the inter-segment shutdown signals and simplifies the "Watchdog Diagnostics" modification installed in January 2014[2].
5. Improved operator interface for improved human factors:
    a. Re-arrangement of operator panel placement to better reflect the operating modes of the accelerator PPS segments.
    b. Improved and consistent operator panel graphics, wording, font and line weights.
    c. Added status lamps for "POWER PERMIT MAGNETS" to the HEBT, Ring, and RTBT PLC-B segments to provide better status feedback and diagnostics to operators.
    d. Moved the Chipmunk radiation monitor HMI control panel closer to the PPS access control and operations workstation.

1 *See USI 102030103-ES0047 "USI Evaluation for the PPS Redundant 24 Volt Power Supply Failure."*
2 *See USI 102030103-ES0049 "USI Evaluation for the PPS Power Supply Wiring Modifications and Implementation of Watchdog Diagnostics to Mitigate Common Mode Failures."*

6. Improved Safety and Maintainability
    a. Consolidated all 120VAC equipment into one rack to minimize potential exposure to dangerous voltages.
    b. Improved wire numbering and color coding
7. Updated the PPS-EPICS Ethernet switches from unmanaged to managed switches consistent with those used by the SNS Controls Networking group for improved cyber security management. These switches are for operator displays only and do not route any safety related signals.
8. Update the 15 CCR PLC controllers from the obsolete model L61 to the manufacturer's recommended replacement model L71.

Items 1 through 3 reflect returning the CCR PPS to the proven pre April 2013 installed system architecture and eliminating the identified common mode vulnerability. Items 4-7 reflect minor beneficial improvements to reliability, safety, human factors, and cyber security identified during the design process. Items 8 and 12, below, address obsolescence of the PLC processor used in the old system. This particular change would have to be made in the near future regardless of the PPS rack replacement project. However, this project provided an ideal test platform to thoroughly verify the manufacturer's recommended replacement worked with the existing hardware and field devices.
There are no changes to the functionality or safety functions performed by the accelerator PPS systems as described in the FSADs Sections 3 and 5 nor the SNS Accelerator Safety Envelope (ASE). Rather, this change increases the reliability and effectiveness of the PPS in performing the safety functions and requirements described in the SNS FSAD and ASE documents.

II.B Summary of Changes to PPS PLC Programs and Configuration

Hardware Changes described in 4 and 5.c, above, require corresponding changes to the mapping of logical to physical inputs and outputs. Changes to the PLC program configuration for the 15 CCR PPS PLCs to support the new rack wiring and PLC model consists of:

9. Remapping Input/Output addresses associated with changing from a standard output module to an isolated output module
10. Remapping Input/Output addresses associated with segregating safety important and non-safety important signals
11. Removal of watchdog handshake signals eliminated by consolidating signals important to safety
12. Update PLC project firmware from the obsolete version 16 to the supported version 21

There are no changes to the PLC logic or functional performance of the PPS systems in order to implement the above configuration changes.
Items 9 through 11 are required to implement the changes described in #4, above. Items 8 and 12 are required due to obsolescence of the present PPS PLC model and firmware used in the present CCR PPS system. The existing PLC model and firmware revision are no longer supported by the manufacturer. The PLC manufacturer verifies the new PLC model and firmware are functionally equivalent to the existing models.[3] The new model addresses non-safety related performance, security, and reliability issues identified in the existing model. Although none of these issues is identified as safety critical at this time, lack of vendor support for the existing PLC would leave the PPS vulnerable to performance and security issues with no recourse available though the vendor.

3 See PCR SNS-RAD-ICS-CM-0142 "Replace L61 with L71."

II.C **Background**

There are seven protection system racks in the CCR. Each rack provides the main accelerator operator interface, system status, and alarms for each SNS operational segment. A cabinet number, i.e. CAB01 – CAB07, designates each rack. CAB01- the Target Protection System (TPS) CCR status and alarm panel - and CAB02 – the Linac Oxygen Deficiency Monitoring status and alarm panel - are not part of this modification.

CABs 03-06, the focus of this change, house the operator controls, status indicators, and redundant Programmable Logic Controller chassis (PLCs)[4] for the Linac, HEBT, Ring, RTBT, and Target PPS segments. The PPS division A PLC chassis for each segment also houses the 'C' PLC for each segment. The five 'C' PLCs are used to perform chipmunk radiation monitoring calculations then pass signals to the division A PLC by hardwire interface.

> *Note: The chipmunk alarm relay contact is independently monitored by the PLC B division for each PPS segment. The B PLC can trip the beam on a radiation alarm independently from PLCs A or C.*

CAB06 presently houses thirty 24VDC power supplies that power each PLC individually. CAB07 houses the access control key panel and PPS entry station video monitors.

The PPS cabinets are co-located for several reasons, one of which is to facilitate sharing hardwired PLC-to-PLC handshake status information that includes inter-segment operating status. This hardwire handshake function is intended to isolate the sending and receiving PLCs in accordance with FSAD-PF 3.2.3.1 *"Overall Scope of PPS and ODH System:"*

> *"Each PPS segment is independent of the other segments such that modifications or repairs to one segment do not affect the other segments."*

And FSAD-NF 3.3.8.3.1.5 *"System Architecture:"*

> *Signals are communicated between the target PPS equipment and the accelerator facility segments via hardwired input and output signals. These signals are designed to be fail-safe. In the event of a power loss, broken wire, or out-of-range signal, the equipment will go to a safe condition.*

In April 2013 change request PCR 1909090101-CM-0022 added redundant DC power supplies for each PLC and connected them through 15 hot-switchover power redundancy modules. Part of this change required connecting all DC power returns together and to the rack earth ground. An unintended consequence of this change was to provide a return path for DC power through the rack earth ground.

The July 2013 discovered common failure mode, described in USI 102030103-ES0047, used the earth ground to provide a return path for an otherwise open circuit return for some, but not all DC power supplies. The DC return was open circuit due to a misplaced clip used to connect DC return wiring terminals together. The difference in potential between the positive power for some inputs and the alternate ground return path was enough to bias inputs to an "ON" state regardless of the status of the associated sending output module. The unintended bias path, known as a 'sneak circuit,' was complicated and depended on several conditions to be true. One condition was that a minimum number of properly grounded outputs had to be ON to create the condition. In the existing design, less important outputs like status lamps, were interspersed with the more important outputs such as inter-segment handshakes. This

4 A PLC is an industrial controller designed specifically for fail-safe high reliability operations in a harsh environment. It is typically composed of a CPU running user logic, inputs to monitor signals, outputs to control devices, and internal and external communications. Internal communications are used to securely route inputs/outputs from the CPU logic to field devices. Separate, external communications are used to route status to read-only user displays (EPICS).

was a remnant of the incremental expansion of the PPS during SNS construction and phased commissioning. The multiple status lamp outputs contributed to the current available to bias the inter-segment handshake inputs. Because the DC returns for both divisions of the redundant PPS were connected through rack ground, both divisions were affected by the failure mode.

The January 2014 interim modifications improved the DC power wiring to make it much less susceptible to open returns. However, all returns remain connected to each other and to rack earth ground. The January 2014 modifications also added a hardware/software watchdog diagnostic function that monitored the inter-segment connections to detect inputs biased to a persistent "ON" state. The Watchdog detects if the inter-segment inputs were stuck ON for any reason and initiates action to shut down hazardous devices.

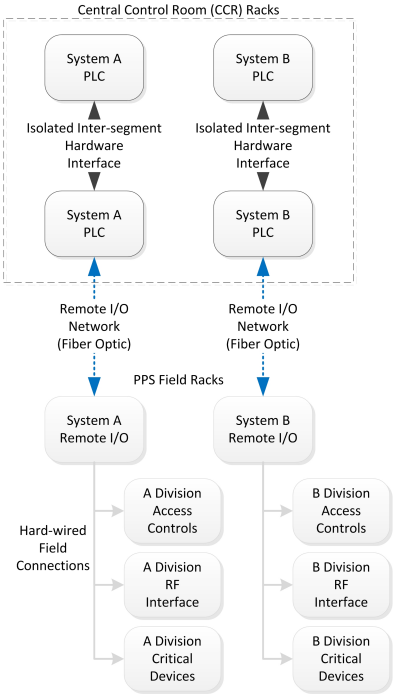
The proposed change described in this USI, part of the long-term corrective action plan, eliminates the common failure mode by completely isolating the PPS division A power from the division B power as well as isolating both divisions from earth ground. The change evaluated in this USI better meets the intent of FSAD-PF 3.2.3.4.1 *PLC Hardware:*

> *"Each redundant PLC in a one-out-of-two configuration is maintained as a separate system to minimize common mode failures."*

Protection Systems engineers determined that the watchdog function continues to add value in detecting an input error regardless of the cause. This function will remain in the new PPS racks. However, due to consolidation of safety critical signals, only 23 of the existing 42 watchdog diagnostic signals are required in the new design.

The scope of this change is only the PLCs and associated wiring in the SNS Central Control Room (CCR) racks. Figure 1 shows the architecture of the accelerator PPS system. No PPS field I/O or devices interfaced to the PPS are affected. Although the PPS systems interface to devices throughout the accelerator, connection to these remote devices (remote I/O) is through a proprietary controls network as described in FSAD-PF 3.2.3.4.1 PLC Hardware:

"Inputs and outputs (I/O) to the PLCs are scattered throughout the facility. For this reason, the remote PLC I/O



SNS-OPM-ATT 2.B-10.a. (Y)

Figure 1 The scope of this change includes the CCR racks only. Remote I/O and field connections are not affected.

modules are connected to the PLC processor via SNS standard industrial control networks."

Appendix 1 is an FMEA evaluating potential failure modes of the proposed isolated DC power modification. The result of the FMEA is there are no negative impacts to the likelihood or consequences neither to the PPS's credited control functions nor to accidents described in the FSADs and ASE. The result of this modification is to improve the accelerator PPS's ability to reliably meet the requirements and intent of the FSADs.

II.D Detailed Description of Changes:

The following section provides more detail on the proposed modifications described in section II.A and II.B

1. *Isolated DC power returns between each PPS division (A/B) and from earth ground to eliminate the common mode vulnerability discovered in July 2013.*

   This change directly addresses the identified common failure mode of sneak paths through interconnected DC power returns within a redundant system.

   - Isolating the PLC A and PLC B 24 VDC power supply commons from each other ensure each of the redundant legs of the PPS operate independently.
   - Isolating the PLC A and PLC B 24 VDC power supply commons from earth (rack) ground will eliminate the potential for a common mode sneak path between the two separate divisions.

   The DC returns were isolated by engineering re-design of the DC power distribution within the CCR PPS racks. Figure 2 shows the existing wiring configuration with power supply commons tied to earth ground. Figure 3 shows the modified power wiring configuration and simplified power supply architecture discussed in (3), below. The revised power supply wiring is fully documented through approved revision controlled drawings.

   Verification:
   The isolation between each of the PLC A and PLC B power supplies and from earth ground was verified through:

   - review of the proposed wiring design
   - independent inspection of the constructed equipment
   - electrical measurements on the constructed equipment
   - proof tests including shorting the +24VDC and the 24VDC return for each supply to earth ground

2. *Replaced DC return shorting clips with a power distribution block.*

   This modification eliminates the direct cause for creating an open return path discovered in July 2013 – a misplaced jumper clip. Figure 2 shows an example of the existing and the new power distribution system. The new power distribution blocks are specifically designed and manufactured for power distribution in industrial control systems.

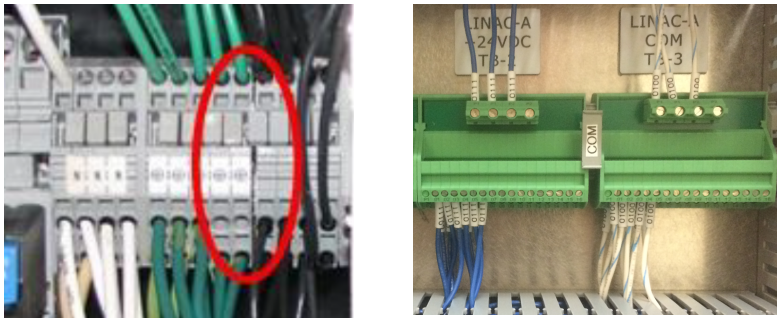


Figure 2 Left: Old CCR Rack method of creating a bus using clips. Clip leading to the common mode failure is circled in red. Right: New CCR rack power and common distribution with purpose built power distribution blocks.

3. *Replaced the 30 redundant DC power supplies and 15 redundancy switchover units installed in April 2013 with 6 isolated DC power supplies.*
   In the existing racks, 30 DC power supplies power the 15 PLCs in a hot-standby arrangement. Each supply is rated at 24V/5A or 24V/2.5A. The load for each PLC and associated inputs and outputs was both calculated and measured in the existing racks. The max load was estimated at 2A and up to 1.5A was measured.
   The new power supply architecture greatly reduces the complexity and potential failure modes of the PPS power distribution with minimal impact to system availability. Instead of two 5A or 2.5A standard power supplies per PLC, the new arrangement uses one 10A power supply. The calculated worst case load is 2.5 A and was measured at 2A during testing with all loads and lamps operating.
   a. Replacing 45 modules with six higher capacity power supplies from the same manufacturer's series (Sola-SDN):
      i. reduces the complexity and potential failure modes of the PPS power distribution
      ii. potentially decreases the SNS machine availability by 0.012%[5]
      iii. decreases the heat dissipation by 60%

   Verification
   The sufficiency of replacing the hot-standby power supply arrangement with standard power supplies was verified through:
   - Engineering design and peer review
   - Verifying the theoretical and actual load for the existing power supplies
   - Selecting a replacement power supply within the same family (Sola-SDN)
   - Selecting a replacement power supply with sufficient overhead and de-rating to reliably power the designated loads
   - verifying performance, isolation, and EMI properties of the selected power supplies
   - independent inspection of the constructed equipment
   - electrical measurements on the constructed equipment
   - proof tests including shorting the +24VDC and the 24VDC return for each supply to earth ground

5 Assuming a power supply failure will drop the PPS to Restricted Access and the mean time to repair and recover full power beam of 12 hours.

4. *Re-arrangement of certain PLC inputs/outputs to separate important signals like inter-segment status and less important signals like panel lamps.*
   This modification improves the reliability of the inter-segment shutdown signals and simplifies the "Watchdog Diagnostics" modification installed in January 2014.
   Twenty-five Allen Bradley 1756-OB16D output modules will be replaced with nineteen 1756-OB16I and nine 1756-OB32 output modules.
   a. The nineteen 1756-OB16I are isolated output modules used to replace modules used for inter-segment handshake outputs. This change is part of the recommendations to eliminate the identified common failure mode. Using individually isolated outputs prevents the output modules from serving as a current source that could potentially bias inputs to the ON state.
   b. Each unique path used for inter-segment handshaking requires a watchdog handshake to assure that path is uncompromised. By consolidating the inter-segment handshake signals, the number of required watchdog diagnostic handshakes is reduced from 42 to 23.
   c. The nine 1756-OB32 are standard output modules used for non-critical functions such as lamps. All outputs not associated with inter-segment handshaking and associated watchdog timers are consolidated into a standard output module within a given PPS segment. This reduces the likelihood a non-critical signal could negatively impact a critical signal, e.g. input short circuit to +24VDC.

   Verification
   - engineering design
   - engineering peer review
   - vendor verification
   - documentation of the PLC module layout
   - wiring documentation for each interface
   - Incoming parts subjected to incoming inspection before release for manufacturer's assembly

   Note: the above change necessitates the re-mapping of I/O names and eliminating unused watchdog diagnostics described in 9, 10, and 11, below.

5. *Improved operator interface for improved human factors:*
   a. *Re-arrangement of operator panel placement to better align with the operating modes of the accelerator PPS segments.*
   b. *Improved and consistent operator panel graphics, wording, font and line weights.*
   c. *Added status lamps for "POWER PERMIT MAGNETS" to the HEBT, Ring, and RTBT PLC-B segments to provide better status feedback and diagnostics to operators.*
   d. *Moved the Chipmunk radiation monitor control HMI closer to the PPS access control and operations workstation.*

   During the design phase, engineers identified an opportunity for improvements to the PPS operator panel locations and graphics. During SNS installation and commissioning, PPS operator panel locations were added to sequentially fill the available rack space. The new panel locations better reflect the operational segmentation for the SNS accelerator. Similarly, small differences in text font, graphics, and signal names evolved over the SNS installation and commissioning period. The new panels use standardized names, font, and graphics. The new arrangement of the front panel retains the original functionality, allows for more efficient use of panel space and improves consistency of the operator interface with the equipment.

Table 1 PPS Panel Relocation

PPS Panel	Old Panel Location	New Panel Location
Front End	CCR03	CCR03
Linac	CCR03	CCR03
HEBT	CCR04	CCR03
Ring	CCR04	CCR04
RTBT	CCR05	CCR04
Target	CCR05	CCR05
Chipmunk HMI	CCR03	CCR06

The present PPS panels for the HEBT, Ring, and RTBT do not have indicator lamps for the PPS division B critical magnets (POWER PERMIT MAGNETS). The PPS division B has the PLC logic for these signals and they are displayed on the EPICS HMI.

Verification

- engineering best practices for human factors
- engineering peer review
- operations review and approval
- panel fabrication and assembly drawings
- inspection and QA

6. *Improved Safety and Maintainability*
   a. *Consolidated all 120VAC equipment into one rack to minimize potential exposure to dangerous voltages.*
   b. *Improved wire numbering and color coding*

   These improvements were to ensure the new racks meet current ORNL standards and practices for electrical safety while eliminating exposure to dangerous voltages where possible. Improvements to the wiring methods helps to reduce installation and maintenance errors that could negatively impact PPS availability.
   Verification
   - engineering best practices for industrial control equipment
   - engineering peer review
   - manufacturer's inspection to UL-508 and NFPA 70E requirements
   - SNS inspection and QA

7. *Updated the PPS-EPICS Ethernet switches from unmanaged to managed switches consistent with those used by the SNS Controls Networking group for improved cyber security management.*
   These switches are used for read-only operator displays only and do not route any safety related signals. This change allows SNS IT to set up and manage rules for EPICS access to PPS read-only signals. It also facilitates rules to ensure only pre-registered and approved devices may communicate on this network. The architecture is compatible with plans for future updates to PPS cyber security controls.
   The PST worked with the SNS Controls and ORNL network support staff to select and implement a switch compatible with SNS Controls network cyber security policy and management tools.

Verification

- Engineering/IT design
- SNS Controls Network Manager's approval
- Lab testing

8. *Update the 15 CCR PLC controllers from the obsolete model L61 to the manufacturer's recommended replacement model L71.*
   The PLC manufacturer has listed the L61 model used in the present system as obsolete and targeted for discontinuation as of December, 2015. The manufacturer's designated replacement is the model L71.
   The L71 has been on the market for three years and is considered a mature product. As with the L61, the L71 is tested and certified for use in safety applications. The major differences between the models is the L71 is faster, has more memory, and has some built-in cyber security features
   Verification
   - engineering equivalency evaluation
   - letter stating equivalency from the manufacturer
   - independent verification in laboratory testing
   - configuration documentation

   Note: the above change necessitates updating the PLC firmware version as described in 12, below.

9. *Remapping Input/Output addresses associated with changing from a standard output module to an isolated output module*
   The conversion to an isolated output module requires revising the PLC tags that associate physical I/O points with logical names used within the PLC program. This process is termed 'remapping' the I/O. The physical I/O point is fixed and defined by the module location and input/output channel on that module. Therefore if the physical I/O changes, the tags in the PLC program must also be changed to ensure the association between the input/output and the tag name remain correct. In updating the tag names, the actual logic functions that use those names are not changed.

   Verification
   - I/O tag name checklists with "before/after" information
   - engineering design
   - independent verification
   - wiring documentation for each interface
   - 100% verification of removals and additions

10. *Remapping Input/Output addresses associated with segregating safety important and non-safety important signals*
    See 9, above.

11. *Removal of watchdog handshake signals eliminated by consolidating signals important to safety*
Because the number of unique inter-segment output module to input module paths is reduced, the number of watchdog diagnostic handshakes reduces from 42 to 23. The PLC logic associated with the 19 eliminated hardwired signals must be removed.

    Verification
    - engineering design
    - Watchdog diagnostic checklists with "before/after" information
    - independent verification
    - wiring documentation for each interface
    - 100% verification of removals and additions

12. *Update PLC project firmware from the obsolete version 16 to the currently tested and supported version 21.*
Replacing the L61 PLC with the L71 requires version 21 or higher firmware. Although version 24 is the highest released version, 21 is the most stable and well tested revision for use in safety applications.
The "software" for a PLC is actually a collection of firmware, user logic, configuration parameters, and variable names (tags) maintained under one 'project' file name. All of the information in a project is keyed to the firmware revision downloaded to the PLC. Keying the project to the firmware revision is the method the PLC manufacturer uses to assure compatibility between hardware and software.
Firmware versions 20 and lower are now obsolete and not supported by the manufacturer; the present CCR PLCs run version 16. Version 20, the highest supported by the L61 processor, has a known issue where in order to communicate with the PLC, one may be required to re-download the PLC program. This action would automatically require a full certification of the affected PPS system. Firmware versions 21 and higher are not supported in the existing L61 PLC. The L71 PLC running firmware version 21 and higher is the only combination that is currently supported by the manufacturer.

    Verification
    - engineering evaluation of revision history
    - manufacturer's recommendation
    - NRTL tests of PLC with V21 firmware
    - SNS laboratory testing
    - independent verification
    - configuration documentation
    - Processes in SNS-RAD-ICS-QA-0001 PPS SQA Plan and SNS-RAD-ICS-PR-0014 PPS SQA procedure.

II.E QA, Verification, and Validation

Given the externally reviewed and approved solution to eliminate the common mode ground error is to isolate the DC power, there are a set of processes in place to ensure the solution and other modifications are implemented faithfully and correctly. 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. Table 2 is a complete list of QA, Verification, and Validation records generated for this project. The list contains five basic types of records:

- Results of Test Procedures
  - Off-line Test Procedures
    - Acceptance tests
    - Integration tests
  - On-Line Test Procedures
    - Commissioning (verification) tests
    - Certification (validation) tests
- QA Reports
- Configuration Management Records
  - Permanent Change Requests
  - Equivalency Review
- Completed Acceptance Criteria Lists
- Completed Equivalency for substituted parts

The list does not include documentation design baseline records such as drawings, engineering notes, and specifications generated in detailing the design process.

II.E.1 Design Process:

Isolation of the 24VDC power for each PPS rack was identified and approved as the appropriate corrective action to eliminate the identified and failure mechanism. Using an isolated output module for important hardwire handshaking was further recommended as a means to reduce similar failure modes. A December 2013 design review of the proposed interim and long-term modifications identified

> *"The long term modifications, isolating all PLC power supplies from earth ground, maintaining segment and chain power supply isolation and using isolated outputs is a correct solution to the original design shortcomings."*[6]

An independently lead SNS Hazard and Operability Study (HAZOP) team tasked with looking for other potential common failure modes also recommended:

> *"The long term corrective action to separate PPS power supply commons remains the best way to eliminate the failure mode leading to the July 2013 event. This will be a multi-year effort."*[7]

The design process first entailed a100% verification of the documentation, construction and wiring of the existing CCR racks. The verified information was then used as the design basis for the subsequent engineering modifications for the new racks. This process ensured the form, fit, and function of the new racks met the requirements of the existing PPS implementation.

6 SNS-RAD-ICS-TR-0002 *"Spallation Neutron Source Personnel Protection System Modification Review Committee Report"*
7 Mahoney, K., et. al. *"Hazard and Operability Study: SNS Personnel Protection Systems."* May 7, 2014

PST engineers developed and tested a representative sample of the proposed modification. The proposal was reviewed by PST and ICS engineers and tested in the laboratory. The modifications were then incorporated into new wiring diagrams for all cabinets. In addition to electrical drawings, the project created assembly, detail, and fabrication drawings for the new rack construction. In all, 119 new revision controlled drawings were generated to document the new CCR racks.

II.E.2 Implementation Process:

II.E.2.1 Hardware Fabrication

A complete set of fabrication and assembly drawings was created as part of the design process.
The PST selected a local vendor to construct, populate, and wire the new racks. The vendor is ISO 9001-2000 certified with significant experience building racks to ORNL standards. The racks were built and inspected to UL 508 and other applicable NRTL standards as required by ORNL SBMS policies.
SNS procured all components and performed incoming QA and test before sending them to the vendor for rack construction.

SNS personnel including the PST staff, designer, and QA representatives visited the vendor facility approximately once per month to assess progress. Any corrections or clarifications were identified and corrected; associated revision-controlled documentation was updated as necessary.
Once delivered the racks were re-assembled for integration testing.

II.E.2.2 Software Modification
The scope of software modifications is limited to the re-mapped I/O addresses and deleting unnecessary Watchdog diagnostic handshake signals removed by consolidating inter-segment signals to isolated output modules.
There are no software modifications that affect the functionality or credited safety functions described in the FSADs.
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 PPS racks.

The PLC software modification process included the following:

- Creation of before/after checklists for modified I/O
- Verification of hardware/software/firmware compatibility using the PLC vendor compatibility matrix and vendor engineering support
- Verification of the ability to operate copies of the existing PPS PLC programs on the new hardware configuration
- Modification of copies of the existing PLC programs to effect the required changes in output modules and reduced number of watchdog handshake signals
- Simulated operation of each PPS segment and inter-segment handshaking
- Verification that only the intended changes were made using inspection and the PLC compare utility

II.E.2.3 Integration Process

SNS personnel performed hardware and software integration testing during the laboratory test phase. 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 CCR PPS with remote I/O devices before commissioning and certification.

II.E.2.4 Operations Documentation and Training

Operations documentation was reviewed to ensure changes to the panel locations and layout are identified and modified as appropriate. Only minor modifications are necessary. Most operator procedures refer to a panel name, not the panel location. For example, Linac PPS Panel, HEBT PPS Panel ... and not CAB03.

During the planned outage to install the modified PPS racks, the Protection Systems Team will provide training to orient the operations staff to the new panel layout.

II.E.3 Testing and Verification Process:

The purpose of the Verification Process is to confirm that the specified design requirements are fulfilled by the system.

II.E.3.1 Acceptance Testing

Once construction was complete, SNS PST and QA personnel performed formal inspection and acceptance testing at the vendor facility with no significant findings. Minor deviances such as a missing color ring, were noted in the QA inspection report; all noted items were corrected and the racks are now 100% in compliance with the documented design (Table 2 #2). SNS-ICS-RAD-TA-0009 R00 *"APPS New CCR racks acceptance test"* is the record of the completed acceptance test (Table 2, #1).

II.E.3.2 Laboratory Testing

On delivery, the racks were moved to a lab space used for testing over a six week period. During this period each of the PLCs was configured and loaded with a copy of the existing PPS logic to ensure the baseline PPS PLC programs would operate on the new system. The logic was then modified to re-map the input/output as described in II.D.7-11.

Laboratory testing included:

- 100% wiring verification
- Verification of the isolation of the DC power supplies from one another and from earth ground
- Verification that the DC power outputs and returns are unaffected by shorts to chassis ground
- Configuration of each of the PLC chassis
- Configuration and check of all PLC inputs and outputs
- Remapping of PLC inputs and outputs as required by changes to the I/O configuration
- Operational check of all panel controls and status lamps
- Inter-PLC hardware handshakes and watchdog timers
- Ability of the PLC to communicate with a remote communications module
- Ability of the PPS logic to transition between operational states and drop to a pre-defined safe state
- Deep inspection of the PLC logic to verify only the intended modifications were implemented. The PLC software includes utilities to compare two revisions of PLC programs and highlights any differences.

The Lab testing culminated in completion of a formal verification test procedure SNS-RAD-ICS-PR-0036

R00 *"APPS Offline Integration Test for new PPS racks in CCR*" (Table 2 #3)

II.E.3.3 Installation Testing

Installation will commence in late June 2015 during the SNS 2015 summer outage. During the installation period all field devices interfaced to the CCR PPS systems will be locked out in a safe condition and the PPS formally removed from service.

The installed system will undergo four phases of testing:

1. Inspection and test of the racks to verify they are mechanically and electrically safe to continue with the subsequent tests.
2. Initial testing involves verifying basic connections and functionality of the installed system. This includes communication with networked field devices.
3. Commissioning involves informal then formal verification all local and remote connections to the PPS are functioning correctly. The results of commissioning will be recorded in SNS-RAD-ICS-PR-0038 *"APPS Commissioning Test for new PPS racks in CCR – complete system."* (Table 2 #4)
4. Once commissioning is complete, the accelerator PPS will undergo a full certification process consisting of 11 separate procedures. Certification procedures are under the SNS OPM section 3.A-7.4.12A through L. Chipmunk Certification falls under OPM section 2.8-18.7. (Table 2, #12-24)

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 the determination of a negative USI as documented through the negative answers to the guiding questions in parts III and IV. The changes associated with the replacement of CCR PPS Rack Cabinets 03, 04, 05, and 06 do not negatively affect the PPS functions described in the FSADs and ASE. Nor are there new failure modes or potential accidents introduced through this change. Rather, the change described in this document improves the overall safety reliability of the installed accelerator PPS systems.

Table 2 Verification and Validation Documentation Generated During the CCR Rack Replacement

	Doc number	Name	Record Type
1	SNS-ICS-RAD-TA-0009 R00	APPS new CCR racks acceptance test	Test
2	Inspection Report 4-22-15	Inspection Results – New PPS Cabinets Fabricated by DCS Electronics	QA
3	SNS-RAD-ICS-PR-0036 R00	APPS Offline Integration Test for new PPS racks in CCR	Test
4	SNS-RAD-ICS-PR-0038 R00	APPS Commissioning Test for new PPS racks in CCR – complete system	Test
5	SNS-RAD-ICS-CM-0051 rev 00	Replace racks hardware	Permanent Change Request (PCR)
6	SNS-RAD-ICS-CM-0139 rev 00	Replace rack software	Permanent Change Request (PCR)
7	SNS-RAD-ICS-CM-0142 rev 00	Replace L61 with L71	Permanent Change Request (PCR)
8	1395587-ACL-APPS-06 R00	New racks general	Acceptance Criteria List (ACL)
9	1395587-ACL-APPS-07 R00	New racks software	Acceptance Criteria List (ACL)
10	1395587-ACL-APPS-08 R00	New racks version upgrade	Acceptance Criteria List (ACL)
11	1395587-EE-001 R00	Equivalency for L71 controller	Equivalency
12	SNS-OPM 3.A-7.4.12.A.	Initial Steps of Linac Portion of PPS Phase 4.0 Certification	Certification Test
13	SNS-OPM 3.A-7.4.12.B.	Initial Steps of HEBT Portion of PPS Phase 4.0 Certification	Certification Test
14	SNS-OPM 3.A-7.4.12.C.	Initial Steps of Ring Portion of PPS Phase 4.0 Certification	Certification Test
15	SNS-OPM 3.A-7.4.12.D.	Initial Steps of RTBT Portion of PPS Phase 4.0 Certification	Certification Test
16	SNS-OPM 3.A-7.4.12.H.	Initial Steps of Target Portion of PPS Phase 4.0 Certification	Certification Test
17	SNS-OPM 3.A-7.4.12.E.	Overall Operational Checklist for the Front End, Linac and HEBT (excluding HEBT Dipoles) portions of PPS Phase 4.0	Validation Test
18	SNS-OPM 3.A-7.4.12.F.	Overall Operational Checklist for the Entire PPS Phase 4.0 with the exception of RTBT DH13 and the Target	Validation Test

	Doc number	Name	Record Type
19	SNS-OPM 3.A-7.4.12.I.	Overall Operational Checklist for the Entire PPS Phase 4.0, including RTBT DH13 and the Target	Validation Test
20	SNS-OPM 3.A-7.4.12.J.	Certification procedure for the addition of Gamma Blockers to PPS Phase 4.0	Validation Test
21	SNS-OPM 3.A-7.4.12.K.	Certification procedure for the Front End Only Mode of Linac PPS Phase 4.0	Validation Test
22	SNS-OPM 3.A-7.4.12.L.	Certification procedure for testing HEBT Chipmunk 200 and Ring Power Permit logic	Validation Test
23	SNS-OPM 2.H-18.6.	Procedure for Validating the Chipmunk Radiation Monitoring System	Validation Test
24	SNS-OPM 2.H-18.7.	Chipmunk System Certification	Certification Test

II.F.1.1 Validation Process

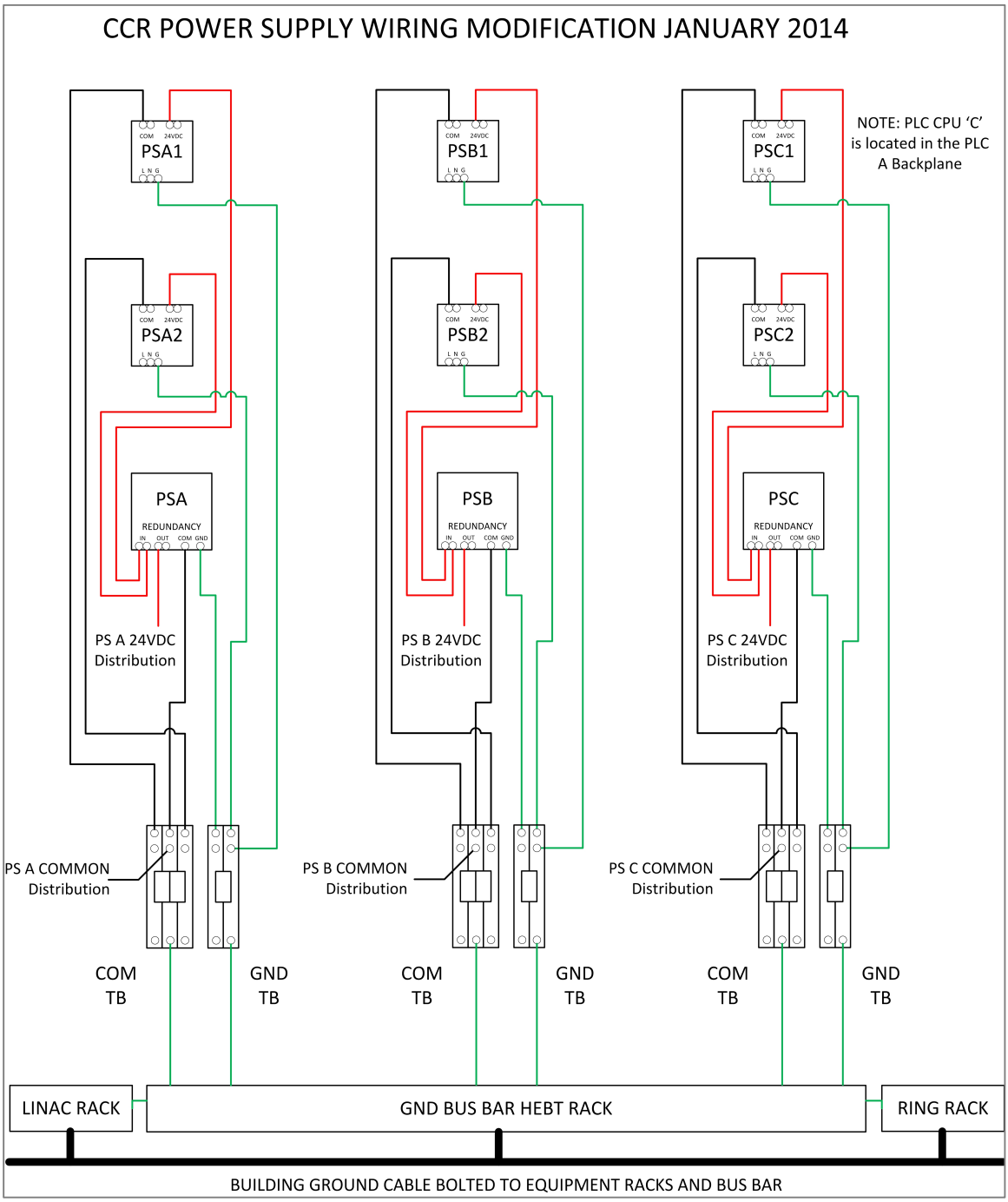


Figure 3 Existing PLC Power Supply Wiring Scheme for a Single Segment (SNS has five segments: LINAC, HEBT, RING, RTBR and Target)

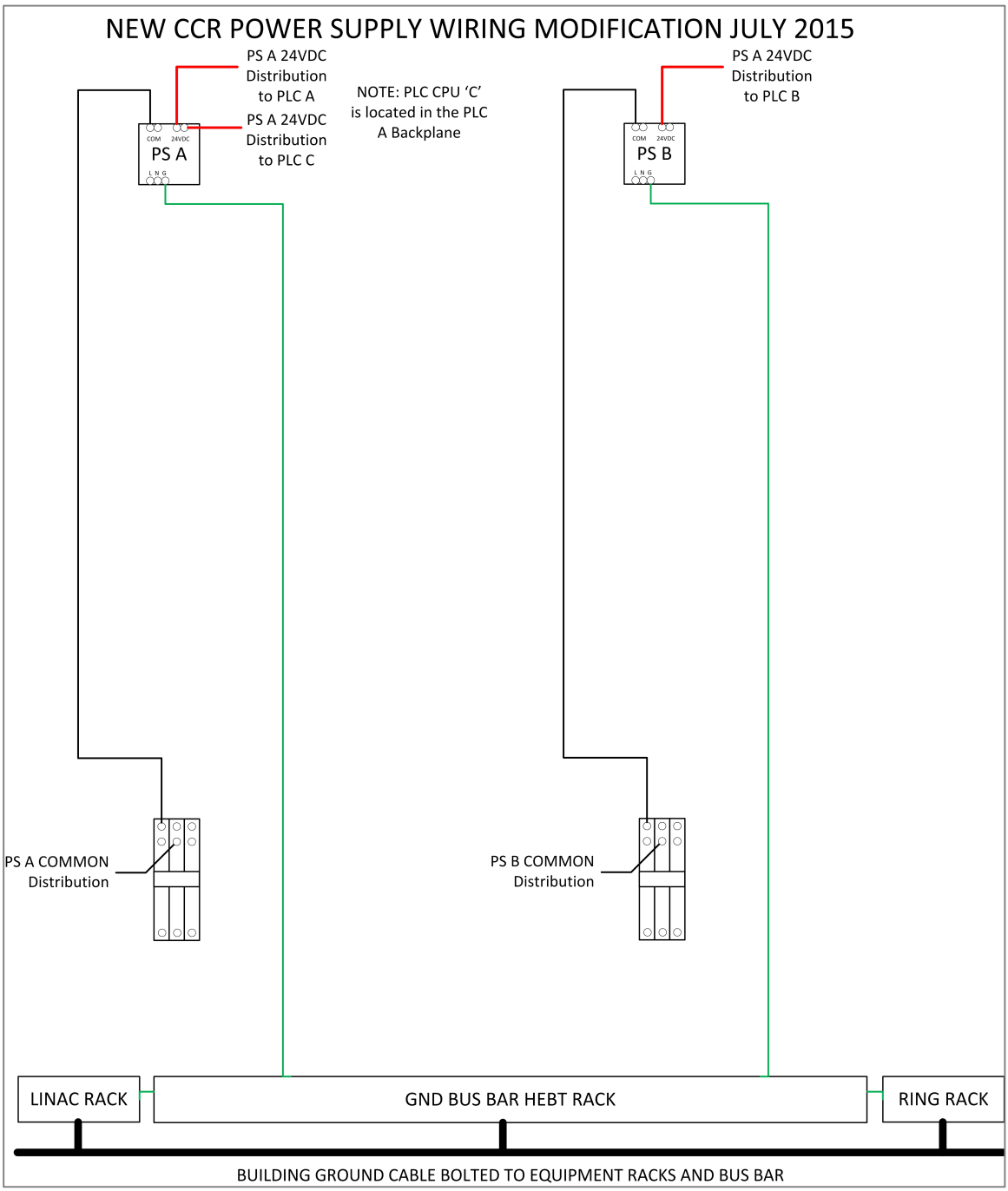


Figure 4 New Simplified Isolated PLC Power Supply Wiring Scheme

Figure 5 Photo of Redundant Power Supplies (30) presently in Cabinet 06. Each group of 3 consists of an A power supply module, B power supply module and C power supply module (from left to right). Each row of 6 power supplies powers one of the PPS segments (Linac, HEBT, RTBT, Ring, and Target). Note that the Redundancy modules are located in the segment racks (Cab 03, 04, 05).

Figure 6 Photo of New Simplified Power Supply Architecture in replacement Cabinet 06. In each row, the left module is Power Supply A and the right module is Power Supply B. The top row provides power to CAB 03, the middle row provides power to CAB 04 and the lower row provides power to CAB 05. The 120 VAC power feeds are at the bottom of the cabinet.

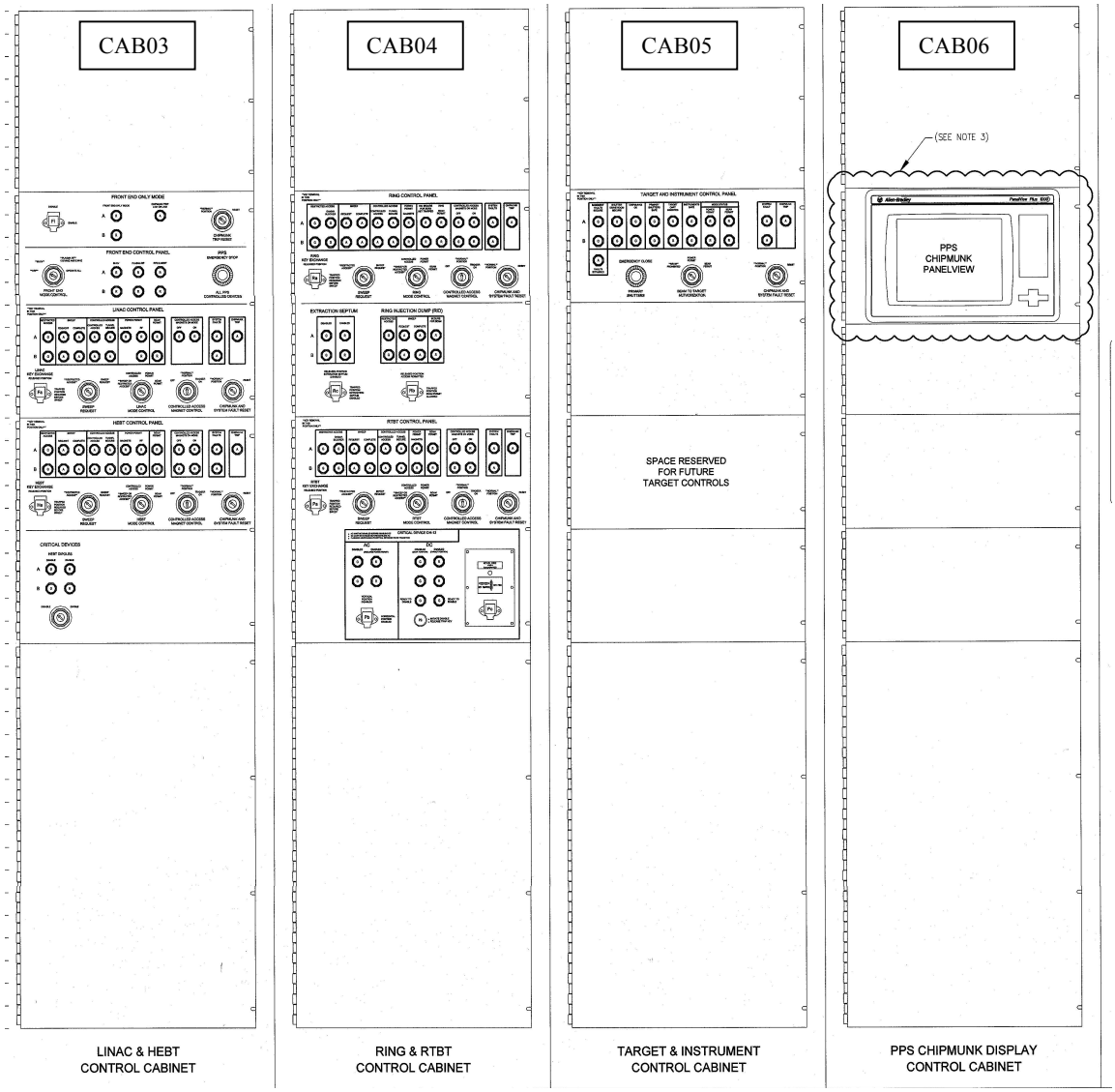


Figure 8 New panel layout for CCR Racks CAB03 - CAB06

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 proposed modifications to the PPS Racks do not affect information presented in the FSADs. The PPS system is described in the FSAD-PF Section 3.2.3 and requirements for the PPS CECs are presented in FSAD-PF Section 5.2.1. Similarly, PPS descriptive information is presented in FSAD-NF Section 3.3.8.3 and requirements for the Target PPS and Instrument PPS are addressed in FSAD-NF Sections 5.2.17 and 5.2.18. The proposed modifications do not affect the safety functionality of the PPS as described in the FSADs other than to remove identified vulnerabilities to a common mode failure. The proposed changes improve the compliance and performance of the PPS within the FSAD requirements. Specifically, the proposed modification better implements the following requirements described in the FSADs:

From FSAD-PF

3.2.3.1 Overall Scope of PPS and ODH System

> *"Each PPS segment is independent of the other segments such that modifications or repairs to one segment do not affect the other segments."*

3.2.3.3 Functional Design of the PPS
3.2.3.3.1 Segmentation
> *"The design of the PPS segments the facility for ease of monitoring and operational organization."*

3.2.3.4.1 PLC Hardware

> *"Each redundant PLC in a one-out-of-two configuration is maintained as a separate system to minimize common mode failures."*

From FSAD-NF

3.3.8.3.1.5 System Architecture
Signals are communicated between the target PPS equipment and the accelerator facility segments via hardwired input and output signals. These signals are designed to be fail-safe. In the event of a power loss, broken wire, or out-of-range signal, the equipment will go to a safe condition.

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

If so, list the affected sections

No, the requirements and operational conditions given in the SNS ASE Section 3.2 *Personnel Protection System (PPS) and PPS-interlocked Area Rational Monitor System* remain unaffected. The level of detail regarding the proposed modifications (e.g. power supply architecture, operator interface with the PPS panels, ethernet switches, etc.) is not addressed in the ASE. The proposed

modifications do not affect the safety functionality of the PPS other than to remove identified vulnerabilities to a common mode failure.

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 PPS is a Credited Engineered Control credited with protecting workers from potentially injurious prompt radiation produced by accelerator operations. The probability of occurrence of an accident associated with accelerator produced prompt radiation is not affected by the proposed modifications associated with the new PPS Racks. The proposed modifications do not affect the safety functionality of the PPS other than to remove identified vulnerabilities to a common mode failure.

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

   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 new PPS Racks. The proposed modifications do not affect the safety functionality of the PPS other than to remove identified vulnerabilities to a common mode failure.

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 main purpose of the proposed modification is to eliminate the identified vulnerability to a common mode failure such that the probability of an unsafe failure of the PPS is reduced.

   Because implementation of the new architecture required fabrication of new racks, vulnerabilities associated with potential deficiencies in design and design implementation are minimized by the design, design implementation, and testing/verification processes described in Section II.E above. Once the new PPS Racks are installed, proper operability of all safety functionality is verified by the completion of the approved full system Commissioning Test followed by a full PPS system Certification in accordance with approved SNS Procedures. The SNS certification procedures are designed to comprehensively verify detailed system functionality. The certification procedures have been matured over the facility's nine-year operating life providing confidence that PPS safety functionality is comprehensively verified.

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 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 other than to remove identified vulnerabilities to a common mode failure.

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 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 PPS 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 PPS other than to remove identified vulnerabilities to a common mode failure.

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 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 will reduce the probability of occurrence of a malfunction of the PPS associated with the vulnerability to a common mode failure.

   The failure modes evaluation presented in Appendix A shows that no new failure modes are introduced by the use of isolated power supplies. Risk associated with design and design implementation are minimized as addressed in the response to Question 3 above.

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.

Kelly Mahoney, PST Team Leader, Qualified Preparer — 1 JULY 2015 Date

Steve Trotter, SNS ESH Environ. Waste Management, Qualified Reviewer — 7/1/2015 Date

David Freeman, SNS Safety Specialist, Qualified Reviewer — July 1, 2015 Date

Aaron Coleman, Cryo Systems I & C Engineer, Reviewer — 7/1/2015 Date

Glen Johns, Accelerator Operations Group Leader, Reviewer — 7-8-15 Date

Approvals:

SNS Operations Manager or Designee — July 8, 2015 Date

VI Appendix A FMEA

Failure Mode	Effect	Mitigation	Detection	Consequence
One Power Supply Return Shorted to Chassis Ground	No immediate effect. Potential difference of 24DC maintained for PPS equipment operation. Shorted system may be susceptible to ground noise and transients. PPS will fail safe if transients trip an input.	1. Redundant isolated power distribution unaffected. PPS safety functionality maintained. 2. Watchdog timer function detects unsafe failure and trips the PPS.	1. Isolation verified during lab testing and during commissioning. 2. PPS PM task to annually verify isolation and nominal Power supply voltage and current.	None PPS safety functionality maintained.
One Power Supply Return Short to Potential < 24VDC wrt PLC supply	Once potential difference is below threshold for PLC operation, affected PLC shuts down.	1. Shutdown is failsafe condition for PPS. 2. Isolated outputs prevent sneak path. 3. Redundant isolated power distribution unaffected.	1. Isolation verified during lab testing and during commissioning. 2. PPS PM task to annually verify isolation and nominal Power supply voltage and current.	Fail-safe shutdown of PPS. PPS safety functionality maintained.

Failure Mode	Effect	Mitigation	Detection	Consequence
One Power Supply Return Short to Potential > 24VDC wrt PLC supply	Potential unsafe failure on one of two PPS chains if voltage exceeds equipment rating. Second chain maintains the safety function.	1. Isolated outputs prevent sneak path. 2. Redundant isolated power distribution unaffected. 3. Power Supply has built-in protection against over-voltage. 4. PPS diagnostics detect momentary signals stuck at '1'; initiates a system fault. 5. Watchdog timer function detects unsafe failure and trips the PPS.	1. Isolation verified during lab testing and during commissioning. 2. PPS PM task to annually verify isolation and nominal Power supply voltage and current.	Redundant PPS division maintains safety function. PPS safety functionality maintained. Watchdog function trips.
PLC Division A Power Shorted to PLC Division B Power	No immediate effect. Potential difference of 24DC maintained for PPS equipment operation.	1. Physical isolation - A and B power are routed to different sections of the racks. 2. Power supplies are designed to work in parallel (load sharing).	1. Isolation verified during lab testing and during commissioning. 2. PPS PM task to annually verify isolation and nominal Power supply voltage and current.	Safety function is maintained.
Missing Ground Jumper Clip – Return Floating (Contributor to original common mode failure)	N/A – Failure mode is eliminated.	Clips are not used for power distribution in new design. New racks have ground bus terminals per accepted good practice.	N/A	None

Failure Mode	Effect	Mitigation	Detection	Consequence
EMI Induced on floating power lines (High Impedance)	Noise causes erratic behavior to PLC components.	1. PLC components certified EMI compliant; designed for industrial factory environment. 2. Isolated lines reject common mode noise better than ground referenced (unbalanced) system. 3. Isolated lines not susceptible to conducted EMI. 4. Shielded power cables reject external EMI. 5. Racks bonded to earth ground for electrical safety and EMI shielding. 6. PLC Power is filtered and isolated from field power.	PPS fails safe	None
Open or partially missing return (Contributor to original common mode failure)	There is no common path for the return to create a sneak circuit (alternate path). Circuits with open return fail-safe.	Fail-safe Design	1. Power connections verified during lab testing and during commissioning. 2. PPS PM task to annually verify isolation and nominal Power supply voltage and current.	PPS fails safe. PPS safety functionality maintained.