

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

I. Title of USI Evaluation:

USI Evaluation for PPS Power Supply Wiring Modifications and Implementation of Watchdog Diagnostics to Mitigate Common Mode Failures

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

This USI Evaluation assesses proposed modifications to the PPS intended as corrective actions to remove the vulnerability to a common mode failure due to the power supply grounding circuitry within the Central Control Room (CCR) PPS racks. The modifications are proposed in response to a common mode failure discovered in July 2013 associated with the power supply wiring that resulted in a positive USI Evaluation [1]. The proposed modifications are as follows:

1. Wiring modifications to separate 24 VDC PPS power supplies within PLC racks located in the CCR;
2. Installation of redundant power supply modules for the LINAC PPS Segment; and
3. Addition of a *Watchdog* diagnostic function to monitor communications.

The proposed modifications have been reviewed by an independent review committee [2] and have been determined appropriate for removing the vulnerability to the common mode failure identified to exist in the CCR PPS racks. Additionally, the proposed modifications will be reviewed and approved by the SNS Configuration Control Committee prior to implementation.

II.1 Background

Personnel protection from prompt radiation hazards produced by the Spallation Neutron Source is provided by Personnel Protection System (PPS) as described in the FSAD-PF [3]. The PPS is divided into the following five basic segments (see Figure 1):

1. LINAC (includes the Front End and LINAC areas)
2. HEBT (the HEBT tunnel)
3. Ring (includes the Ring and Injection Dump)
4. RTBT (the RTBT Tunnel)
5. Target (includes the Target utility areas and neutron instruments)

Each segment uses a dual channel (Channel A and Channel B) Programmable Logic Controller (PLC) based system. The segments communicate with each other using redundant Channel A and Channel B PLC Input/Output (I/O) modules. All of the PPS intersegment communications I/O modules are located in the CCR PPS racks. Figure 2 shows a depiction of *intersegment* communications between I/O modules.

A third channel, PLC C, handles Chipmunk signals. The PLC power supplies and Input/Output modules are contained within the CCR PLC A chassis for each PPS segment except for the LINAC segment. The PLC power supplies and Input/Output modules for LINAC Channel C are located in the Front End building. LINAC PPS racks were initially installed in the Front End building prior to completion of the SNS facility. After the CCR was completed, PPS racks were relocated to the CCR; however, the PLC C racks for the LINAC was never moved and remains

in the Front End Building. Therefore the CCR racks housing the LINAC PLC segments contain PLC Channel A and Channel B power supplies but not the PLC power supplies. Additionally, the CCR rack for the LINAC PLC segment also contains the power supply for the Chipmunk Panelview system.

PLC Channel C communicates with PLC Channel A within each segment but does not communicate with any other segments. This communication is referred to as an *intra-segment* communication. PLC C communicates with PLC Channel A and PLC Channel A provides the communication link to the other segments. Figure 3 shows a depiction of an *intra-segment* PLC C to PLC A communication.

During PPS testing in July 2013 it was discovered that the LINAC segment failed to trip as requested by the HEBT segment in both the Channel A and Channel B PLC chains. It was discovered that an improperly installed jumper connection between common and ground resulted in a loss of power supply return path for the intersegments received by the HEBT PLC in the Ring segment which allowed the common buss of the HEBT PLC output modules (both A and B) to float above ground. The intersegment PPS return currents found a sneak path back through the HEBT PPS that raised the output voltage of the HEBT above its “off-state” voltage. This resulted in the HEBT segment communicating a false safe (high) signal to the LINAC segment. This situation is depicted in Figure 4 that shows the improperly installed jumper connector, highlighted in red. Because the improperly installed jumper failed to make the intended connection between the common and ground sides of the terminal block, the common legs began to float above ground causing the unsafe failure.

The jumper was improperly installed as a part of planned work being done to install redundant PLC power supplies in the CCR Rack for the HEBT PPS segment. The redundant power supplies were being installed as a part of an initiative to replace single 24 Volt power supplies with redundant 24 Volt power supplies in the CCR racks for each of the PLC segments. The goal of the initiative was to improve system availability. At the time of the event, redundant power supplies had been installed in all of the CCR PLC segment racks except for the LINAC, which was scheduled to be modified at a latter date.

The event was analyzed and determined to constitute an Unreviewed Safety Issue per DOE Order 420.2C (USI Evaluation 102030103-ES0047-R00 [1]). Investigations determined the cause and that when earth ground was connected to the HEBT commons the system worked as designed. Subsequently, common and ground connections for PLC power supplies in each PPS segment were tested and verified to have proper continuity and intersegment communications were tested and verified to be operational. It was determined that SNS could safely operate on an interim basis with the as-installed power supply configuration that was vulnerable to a common mode failure of a break in the common to ground connection provided certain compensatory actions were implemented that included rigorous configuration control of the PLC cabinets and weekly testing of inter- and intra-segment communications.

The weekly testing of inter-segment communications was based the estimated probability that a single wire or jumper could break or become disconnected either spontaneously or due to some unanticipated and unidentified energetic event. It was determined that “weekly testing” combined with other corrective actions, was sufficient to mitigate the possibility that a single

connection failure within the CCR PPS rack power supplies could render both PLC A and B channels incapable of properly responding to an unsafe condition [1].

A laboratory test stand was assembled to mock up the equipment in order to recreate the event and independent reviewers were consulted. Subsequent investigations have led to a more comprehensive understanding of the issue and have identified corrective actions to address the identified vulnerabilities.

II.3 Wiring modifications to Separate PLC Power Supplies in CCR PPS Segment Racks

As described above, the common mode failure occurred when a single jumper was improperly installed during installation of redundant power supplies into the HEBT PLC segment rack located in the CCR. This work was part of an initiative to upgrade from single to redundant power supplies for each of the PPS Segments. Redundant power supplies have been installed in the CCR PPS racks for the HEBT, RING, RTBT, and Target segments using the same wiring scheme; therefore each is vulnerable to a similar common mode failure. The CCR rack for the LINAC PPS segment has not yet been upgraded to incorporate redundant power supplies; however, investigations show that a similar vulnerability exists within the single power supply scheme of the LINAC segment.

The existing power supply-wiring scheme for the HEBT, RING, RTBT and Target CCR PPS racks is shown in Figure 4. The existing power supply-wiring scheme used for the LINAC PLC segment is shown in Figure 5. Note that the LINAC does not have PLC Channel C power supplies in its CCR rack but does include the power supply for the Chipmunk Panelview system.

The wiring shown in Figure 6 is proposed to eliminate the possibility that loss of any single connection could render both Channel A and B inoperable. The proposed wiring configuration of Figure 6 accomplishes the following:

- Separates PLC A, PLC B and PLC C power supply wiring from each other
- Provides multiple return paths from each terminal strip assembly such that a single wire fault can only affect a single channel (i.e. will not result in a common mode failure)
- Provides redundant earth ground wiring between racks to protect against the loss of earth ground due to a single fault.

Because the single power supply system in the LINAC segment has a similar vulnerability, it is proposed to install redundant power supplies in the LINAC CCR rack in accordance with the wiring modifications described in the section below. Therefore the LINAC CCR rack will be wired in the same fashion as each of the other segments (see Figure 7).

As described above, the LINAC PLC C power supplies are located in the Front End Building and use a different wiring scheme that employees interposing relays for isolation. There are no plans to modify the LINAC PLC C power supplies at this time because the LINAC PLC C power supplies do not have the wiring vulnerability identified in the other power supplies.

Details of the proposed wiring change and subsequent testing to ensure operability have been

reviewed by a committee of independent reviewers and deemed to be appropriate [2]. Detailed wiring for the proposed modifications to each PPS segment is shown in the following approved drawings.

PPS Segment	SNS Drawing No.
LINAC Segment	109090101-R8U-A060
HEBT Segment	109090101-R8U-A081 and 109090101-R8U-A081AB
Ring Segment	109090101-R8U-A101
RTBT Segment	109090101-R8U-A121
Target Segment	109090101-R8U-A139

II.4 Implementation of Watchdog Diagnostic to Monitor Communications

It is proposed to implement Watchdog Timer (WDT) diagnostics within the PPS capable of detecting the type of fault condition discovered July 2013. The watchdog diagnostic will monitor the inter-segment and intra-segment communications and will provide a fault signal to the PLC should a disruption in communications be identified.

As described above, the five PPS segments communicate with each other via intersegment communications as depicted in the simplified diagram presented in Figure 2. Each line depicting communication between segment outputs and segment inputs represents multiple inputs/output communications between the segments. For example, there are 6 unique HEBT PLC output/LINAC PLC input communications (3 for PLC A and 3 for PLC B), all represented by the single arrowed line in Figure 2. A watchdog diagnostic will be added to each unique intersegment PLC output/PLC input pairing for a total of 6 watchdog diagnostics for HEBT/LINAC intersegment communication. The number of watchdog diagnostics associated with communications between segments is indicated in Figure 2. Wiring will be installed to transmit each watchdog signal between modules.

Figure 8 depicts an example of the wiring between a single HEBT output to LINAC input module for a single channel (e.g. Channel A). An oscillating watchdog signal will be transmitted from the output module to the input module across a newly installed wire as shown at the bottom of the diagram.

Programming will be added to each PLC processor to drive a new output signal alternating high and low at a 10 second cycle time. This new output signal will be sent to the corresponding input module in the next segment. Programming will be added to the receiving segment to examine the watchdog output to determine if it is changing state as intended.

If the diagnostic programming detects that an inter-segment watchdog input function has failed then the receiving segment will act to terminate beam operations in an analogous manner as if a real unsafe trip signal had been issued by the output module. All segments of the PPS (except for the Target PPS which does not receive inter-segment inputs) control at least one critical

device as described in the FSAD-PF [3]. Critical device response to a failed inter-segment watchdog signal will be as follows:

Transmit Segment	Receive Segment	Receive Segment Action
HEBT	LINAC	Disable 65 KV PS, RF to RFQ, MEHT RF, HVCMs ¹
Ring	LINAC	Disable 65 KV PS, RF to RFQ
RTBT	LINAC	Disable 65 KV PS, RF to RFQ
Target	LINAC	Disable 65 KV PS, RF to RFQ
Ring	HEBT	Disable HEBT Dipoles
RTBT	HEBT	Disable HEBT Dipoles
RTBT	Ring	Disable Extraction Septum
Target	Ring	Disable Extraction Septum
Target	RTBT	Disable RTBT:DH13

If the diagnostic programming detects that an *intra-segment* (PLC C to PLC A) watchdog input function has failed then PLC A will respond as if a PLC C unsafe trip condition had been transmitted, that is tunnel status will drop from beam permit to power permit mode.

The HEBT segment is a special case because PLC C sends a HEBT Chipmunk Channel 200 status signal to both PLC Channel A and PLC Channel B. This is because Chipmunk Channel 200 is used for special entry conditions and is designed to directly communicate with both PLC Channel A and PLC Channel B. For this special case, a new watchdog signal will be added to both the HEBT PLC C to PLC A and PLC C to PLC B I/O modules. If HEBT PLC A or HEBT PLC B detects a failure of the watchdog signal, then the HEBT will drop from beam permit to power permit.

An intra-segment watchdog signal is not provided for the LINAC segment. In this segment the I/O modules are located in the Front End building and use interposing relays for isolation.

II.5 Testing and System Certification

An integrated testing procedure and PPS certification procedures have been developed to ensure the proposed hardware and software modifications are properly implemented and functional as described in Permanent Change Request SNS-RAD-ICS-CM-0041. The integrated test procedure and PPS certification procedures will be reviewed and approved by SNS line management prior to implementation. The planned testing and validation process to ensure proper implementation integrated testing and PPS certification were reviewed by the independent review committee [2] and determined to be adequate.

The USI Evaluation [1] showed that SNS could safely operate with the as-installed power supply configurations (in the HEBT, RTBT, RING, and Target segments) with the identified common mode failure vulnerability described above provided certain additional controls be put in place:

1. Verifying that all redundant power supplies were properly installed and operable
2. Minimizing access to the cabinets and enforcing strict configuration control of the PPS System, and

¹ LINAC Segment drops to Power Permit, RF disabled

3. Testing system functionality at least once every 18 days.

The proposed modifications as described in this evaluation will remove the common mode failure vulnerability identified in the PPS PLC power supply circuitry [2]. Therefore the controls identified in USI Evaluation [1] are no longer needed because the purpose of the identified controls (listed above) was to ensure reliability while continuing to operate with the known vulnerability associated with the power supply wiring. The weekly testing interval was based on the estimated probability that a single wire or jumper could break or become disconnected either spontaneously or due to some unanticipated and unidentified energetic event. Because the proposed modifications remove the identified power supply vulnerability to a single point common mode failure, the need for weekly testing will no longer be required.

Continuation of regular periodic testing as a part of the required annual certification would; however, be prudent. The independent review committee [2] recommended the following semi-annual testing be implemented:

“Every semi-annual outage verify PLC commons show proper continuity between segments in lieu of inter-segment testing before the long term solution is implemented.”

II.6 Planned Future Modifications

The proposed wiring changes described above eliminate the possibility of the same type of common mode failure discovered in July 2013; however, the design goal for the system is to totally isolate PLC Channels A and B to further minimize unforeseen potential vulnerabilities to a common mode failure. Future planned modifications, not evaluated here, to isolate the PLC power supply commons from earth ground and to install isolated output modules for intersegment communications have been endorsed by the independent review committee [2] to achieve the design goal of fully isolating the two channels.

II.7 References

1. USI Evaluation for the PPS Redundant 24 Volt Power Supply Failure, SNS102030103-ES0047-R00, August 9, 2013.
2. Spallation Neutron Source Personnel Protection System Modification Review, Committee Report, December 3rd and 4th, 2013, SNS-RAD-ICS-TR-002 R00, December 11, 2013.
3. SNS Final Safety Assessment Document for Proton Facilities, SNS 1022030102-ES0016-R03, September 2011.

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 PLC 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”*. Implementation of the proposed modifications described here accomplishes separation of the CCR rack PLC power supplies.

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

The proposed modifications do not affect any of the requirements of the ASE. The ASE provides operability requirements for the PPS in Section 3.2. The level of detail regarding how PLC power supplies are wired is not addressed in the ASE. The proposed modifications as described above will remove the common mode failure vulnerability identified in the PPS PLC power supply circuitry [2].

V. USI Evaluation Criteria:

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

Justification: 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 accelerator produced prompt radiation is not affected by the proposed modifications to the PLC power supplies or the implementation of the watchdog diagnostic.

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

Justification: The PPS is a Credited Engineered Control whose primary function is to protect workers from potentially injurious prompt radiation produced by accelerator operations. The unmitigated consequences (i.e. potential radiation exposures due to an accident without PPS protective actions) are not affected by the proposed modifications to the PLC power supplies or the implementation of the watchdog diagnostic.

3. Could the change significantly increase the probability of occurrence of a malfunction of equipment important to safety previously evaluated in the FSADs?
Yes No

Justification: The proposed modifications will reduce the probability of occurrence of a malfunction of the PPS associated with the vulnerability to a common mode failure due

to the power supply grounding circuitry within the Central Control Room (CCR) PPS segment racks. As described in the text above, implementation of the proposed modifications will remove the need perform the weekly (not to exceed 18 days) functionality test to ensure reliability as identified in the earlier USI Evaluation [1] because the need for the weekly test was to ensure system reliability while continuing to operate with the identified power supply system vulnerability to a single point common mode failure and the estimated probability of a single connection failure. Implementation of the proposed modifications will remove the power supply system vulnerability to a single point common mode failure. Testing during each semi-annual outage to verify PLC commons show proper continuity between segments in lieu of the weekly testing as recommended by the independent review committee [2] combined with required annual PPS certification will provide further assurance of system reliability.

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

Yes__ No

Justification: The PPS is a Credited Engineered Control 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 are unchanged by system modifications.

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

Yes__ No

Justification: 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 proposed modifications consist of power supply wiring modifications; the implementation of redundant power supplies in the PPS LINAC segment; and the implementation of watchdog diagnostics to monitor communications between and within segments. The types of significant accidents associated with the PPS system continue to be personnel exposure to accelerator produced prompt radiation; no new types of accidents are 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

Justification: 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 due to the power supply grounding circuitry within the Central Control Room (CCR) PPS segment racks [2]. The proposed modifications have been reviewed and endorsed by an independent review committee [2]. Additionally, the proposed modifications will be reviewed and approved by the SNS Configuration Control Committee prior to implementation. After the proposed modifications have been implemented, integrated system testing and full PPS certification will be conducted in accordance with approved SNS procedures prior to SNS beam operations. The planned testing and validation process to ensure proper implementation integrated testing and PPS certification has been reviewed by the independent review committee and determined to be adequate. These measures are designed ensure proper system operability after the modifications have been implemented.

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

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



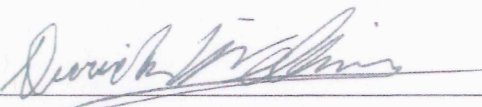
David Freeman, Qualified Preparer
Dec 20, 2013
Date



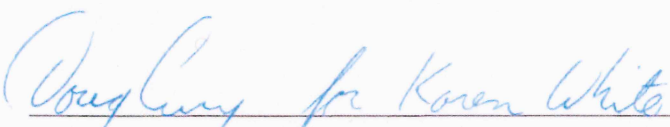
Mike Harrington, Qualified Reviewer
Dec 20, 2013
Date



Paul Wright, PTS Team Leader
12/20/13
Date



Derrick Williams, CF and Vacuum Process Controls Engineer
12/20/13
Date

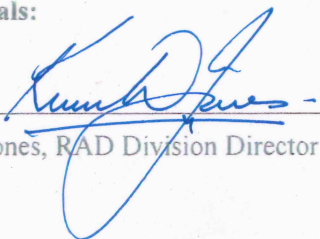


Karen White, Control Systems Group Leader
12/20/2013
Date



George Dodson, Deputy Division Director
20 Dec 2013
Date

Approvals:



Kevin Jones, RAD Division Director and SNS Operations Manager
12.20.2013
Date

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

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

David Freeman, Qualified Preparer

Date

Mike Harrington, Qualified Reviewer

Date

Paul Wright, PTS Team Leader

Date

Derrick Williams, CF and Vacuum Process Controls Engineer

Date

Karen White, Control Systems Group Leader

Date

George Dodson, Deputy Division Director

Date

Approvals:

Kevin Jones, RAD Division Director and SNS Operations Manager

Date

Appendix A. Figures



Figure 1. SNS PPS Segments

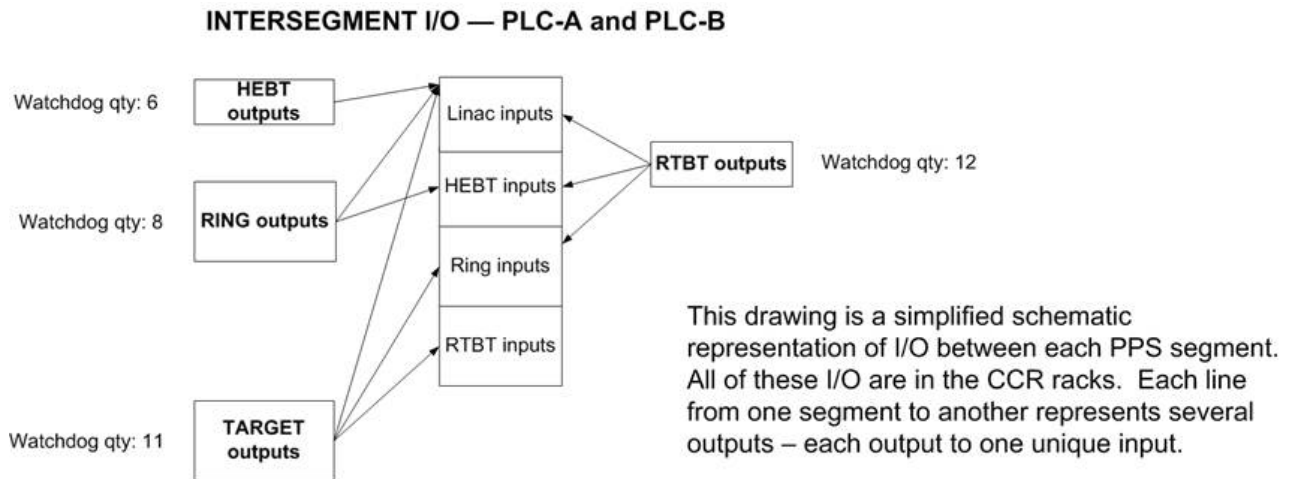


Figure 2. PPS Intersegment Communications

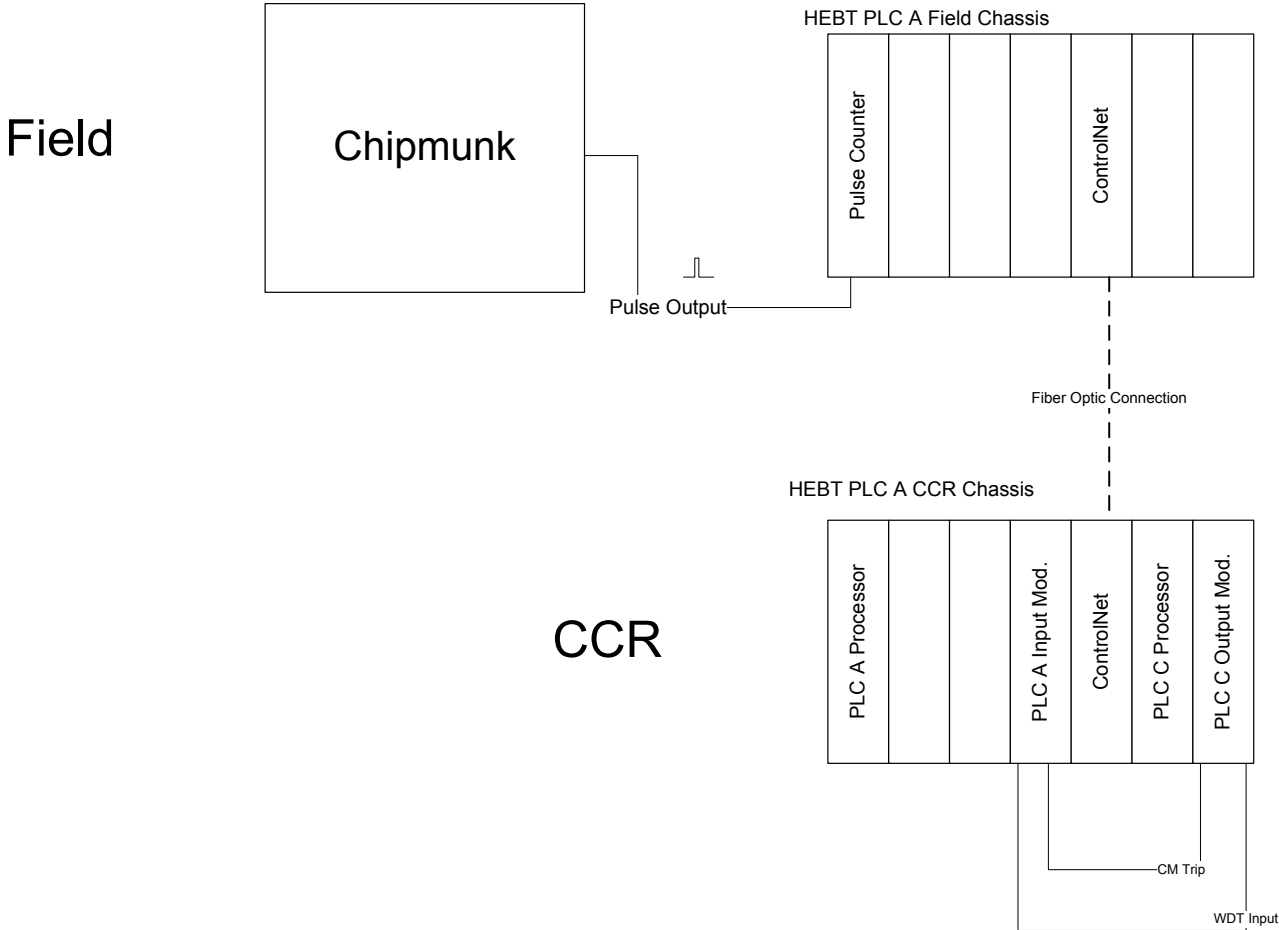


Figure 3. Example of Intrasegment Communication Wiring for HEBT PLC A. (The pulse output of the Chipmunk is communicated through the ControlNet to the PLC C processor which then communicates with PLC A. The Watchdog signal is transmitted by PLC C and carried to PLC A)

CCR HEBT POWER SUPPLY GROUNDING DIAGRAMS

CCR POWER SUPPLY WIRING EXISTING

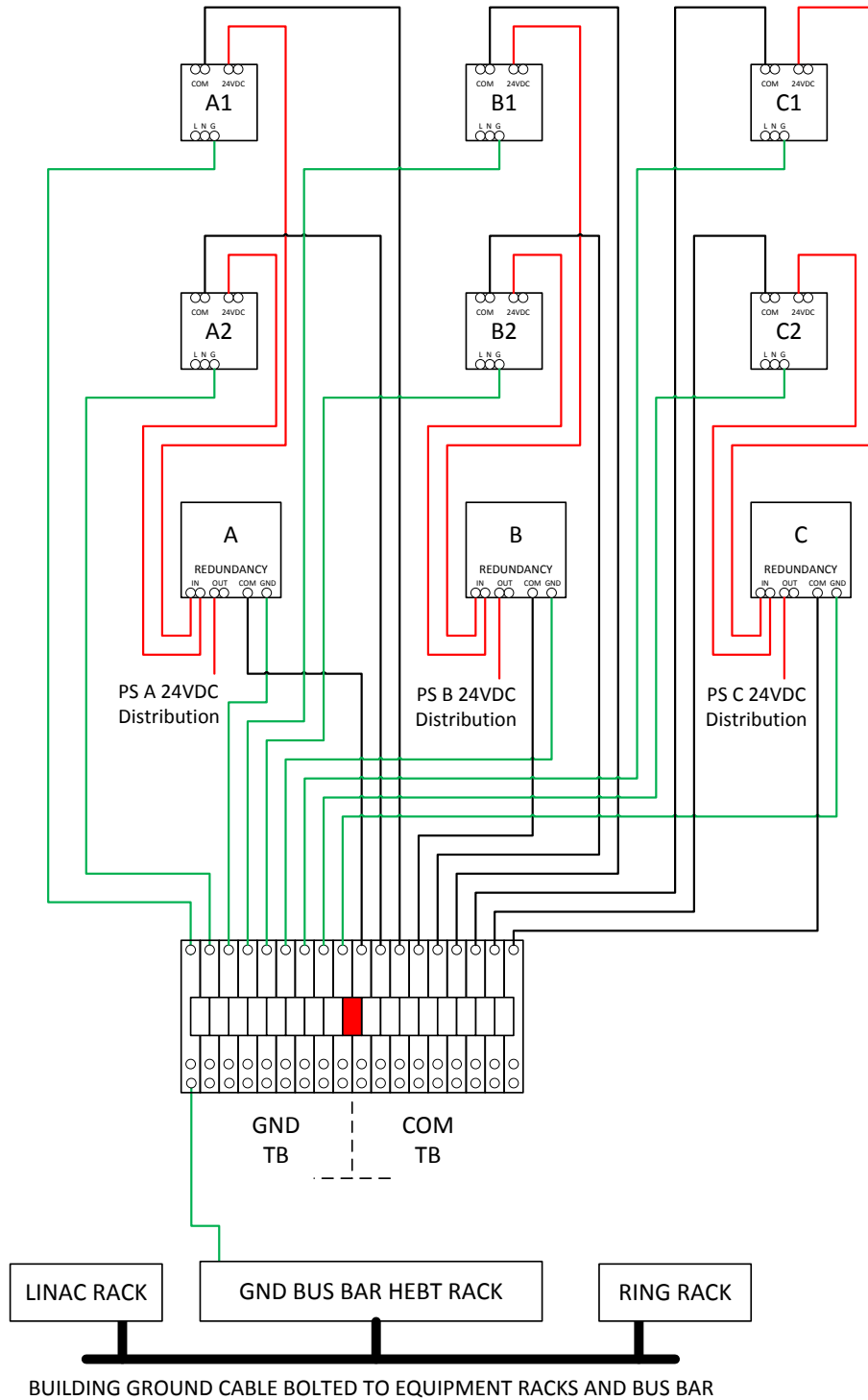


Figure 4. Existing PLC Power Supply Wiring Scheme for the HEBT, RING, RTBT, and Target PPS Segments

LINAC POWER SUPPLY WIRING

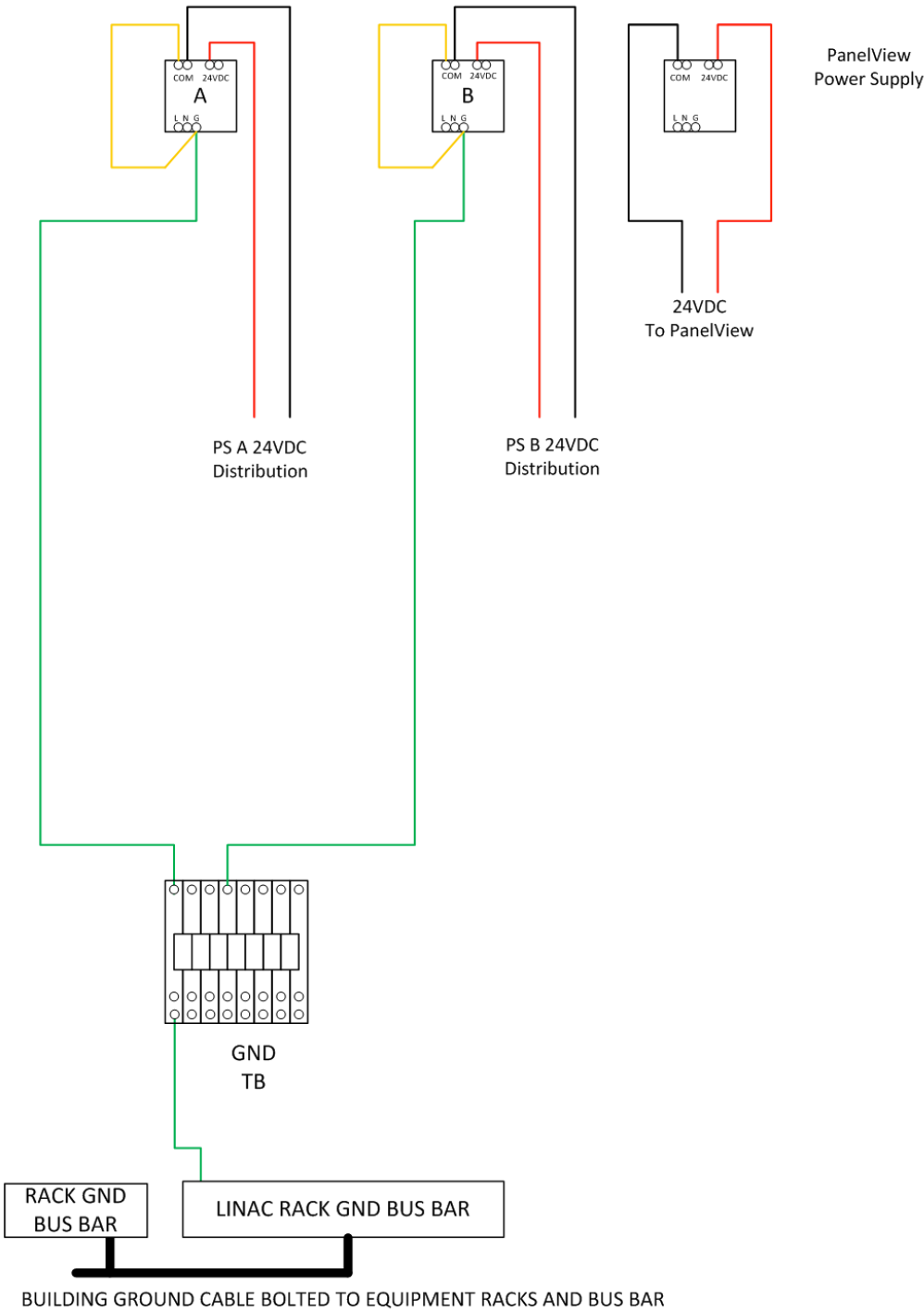


Figure 5. Existing PLC Power Supply Wiring Scheme for the LINAC PPS Segment

CCR POWER SUPPLY WIRING PROPOSED

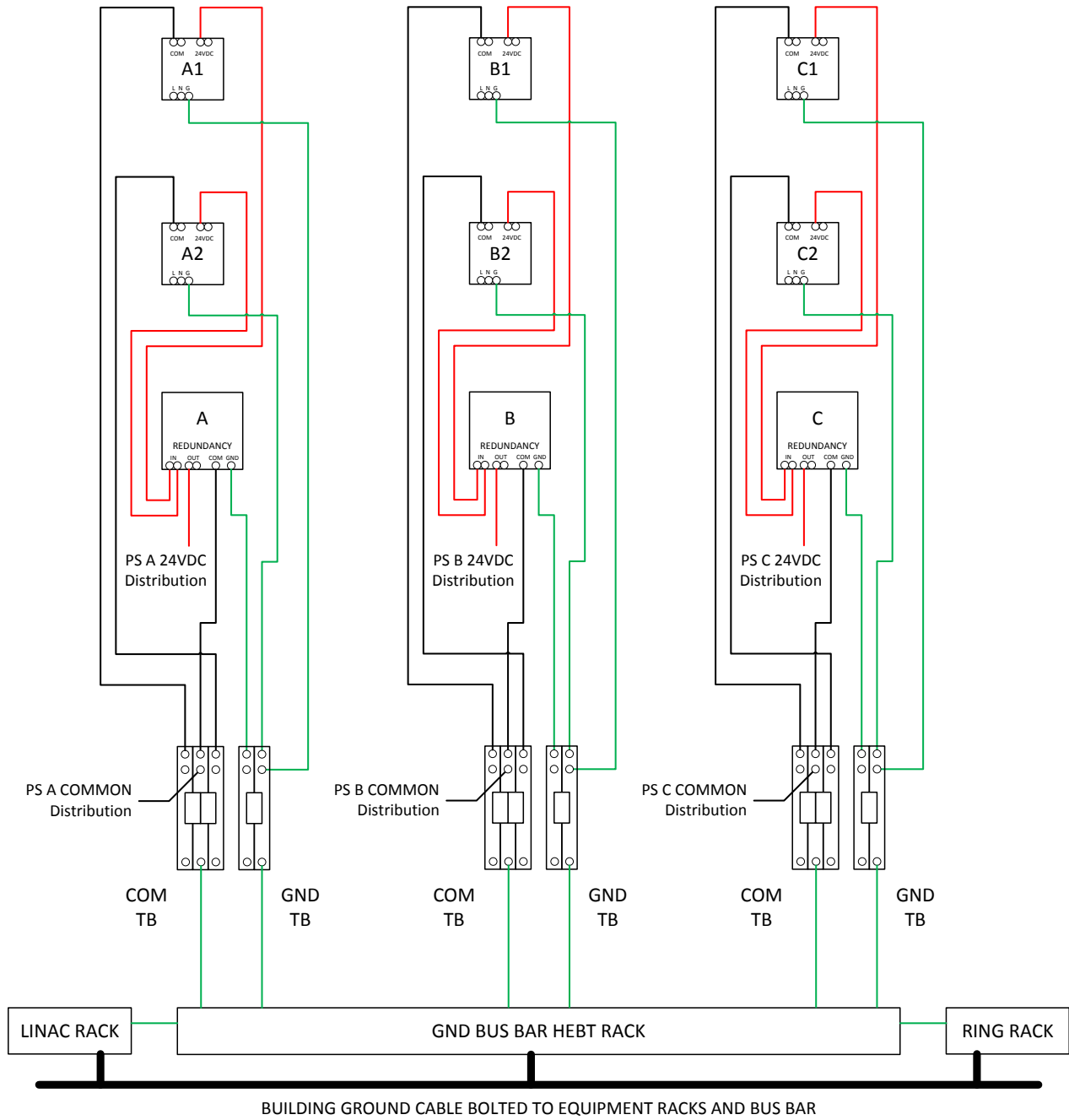


Figure 6. Proposed PLC Power Supply Wiring Scheme for the HEBT, RING, RTBT, and Target PPS Segments

CCR LINAC POWER SUPPLY WIRING PROPOSED

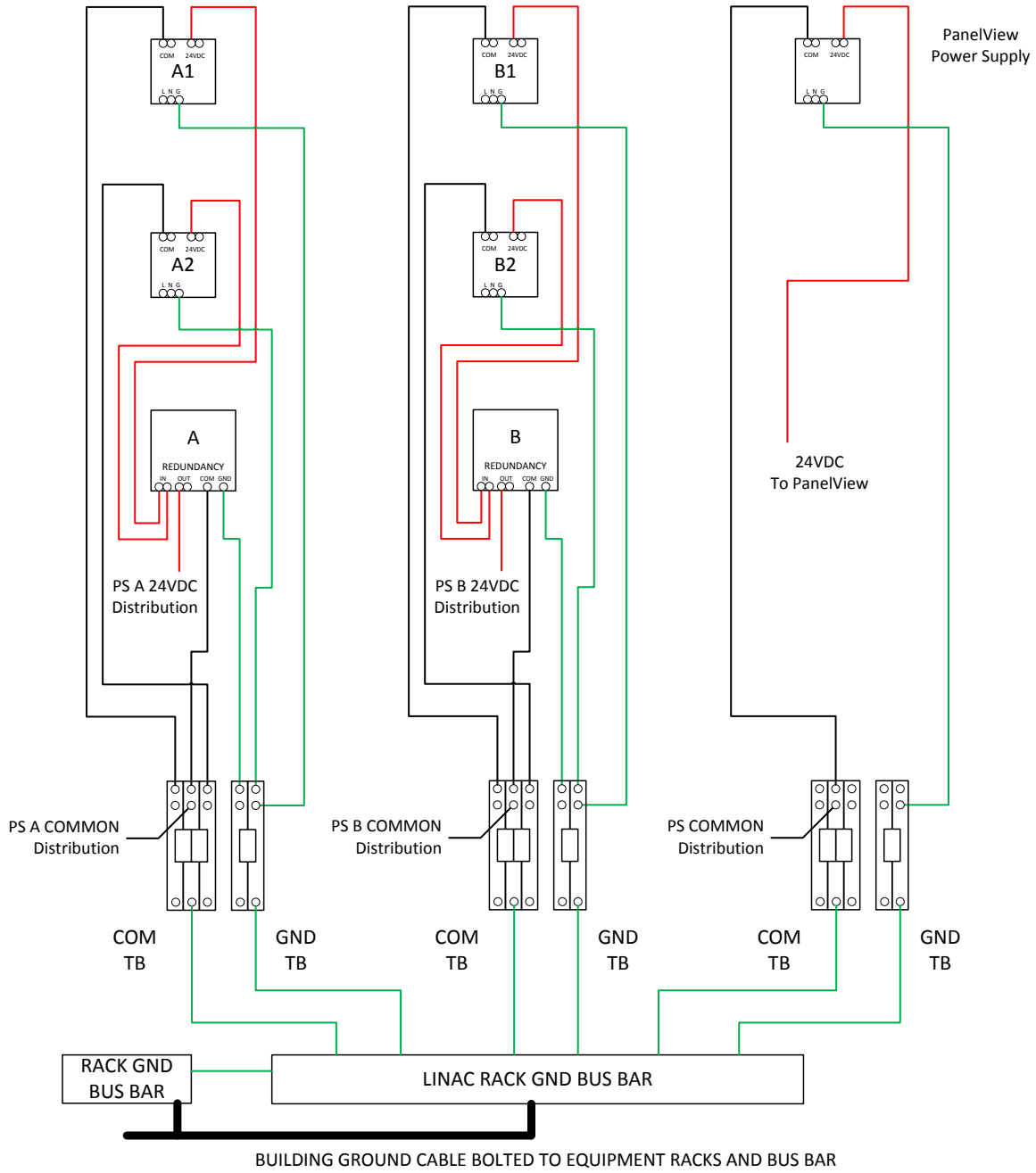


Figure 7. Proposed PLC Power Supply Wiring Scheme for the LINAC PPS Segment

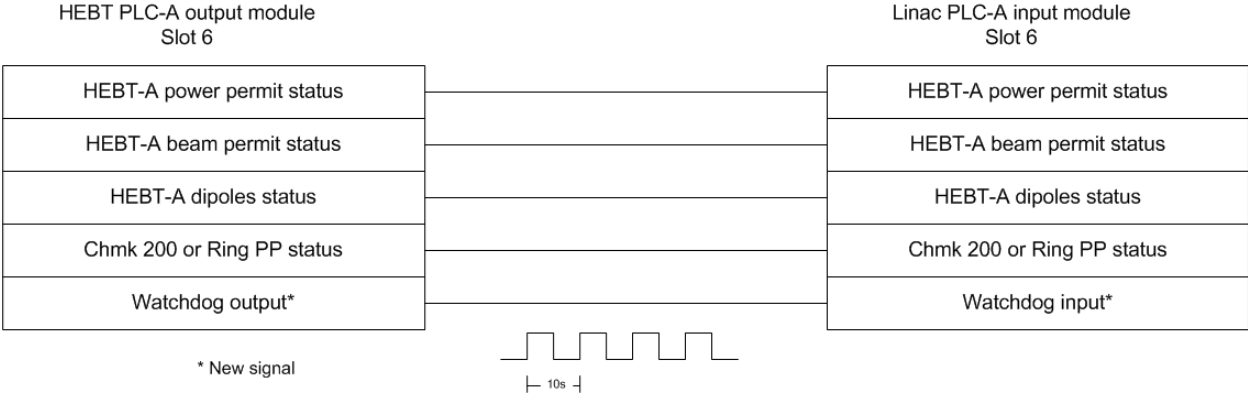


Figure 8. **Example of PPS Intersegment Wiring Between a HEBT and LINAC Module**
(The lower tier represents the proposed watchdog diagnostic.)