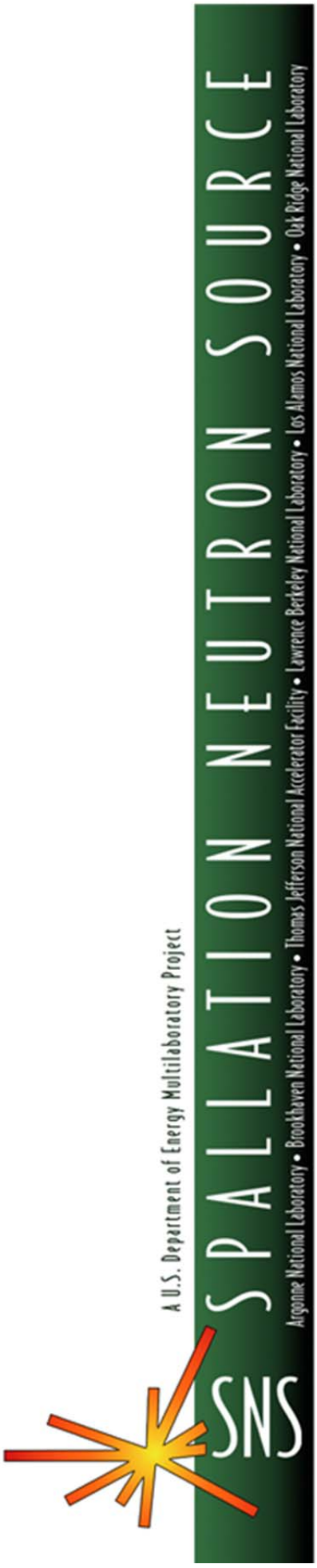
HAZARD AND OPERABILITY STUDY:

SNS PERSONNEL PROTECTION SYSTEMS

MAY 7, 2014



Submitted: 7. MAY. 2014
Kelly Mahoney: Facilitator, Thomas Jefferson National Accelerator Facility

Approved: 5/7/2014
Douglas Curry: Acting Protection Systems Team Leader

Reviewed: 5/7/14
Karen White: Controls Group Leader

Table of Contents

1 Purpose

This report is in response to ORNL ACTS .28733.8 and .28733.9, which refer to ORPS-CHRIDGE-2013-005, #7 and ORPS-CHRIDGE-2013-005, #8 respectively.

On July 31st, 2013 during scheduled certification testing, Protection Systems Team personnel uncovered an unsafe common mode failure of the SNS Personnel Protection Systems (PPS). SNS reported the event to DOE, took immediate compensatory actions, and formed an investigation team. The ensuing investigation and report produced several corrective actions to ensure SNS operations remain safe. The root cause of the common mode failure was inadequate review and testing of modifications to the PPS. The direct cause was an installation error that defeated the ability of one PPS segment to demand a shutdown of the primary beam. The error was such that it defeated both of the redundant PPS chains.

Corrective actions addressing the root and direct cause are complete. This report addresses one of the two remaining corrective actions – perform a failure mode study of the PPS to look for additional undetected common failure modes. The final corrective action is to use the results of this report to plan and implement modifications to the PPS necessary to address critical common failure modes, if any are found.

In the context of this report a 'Finding' is the outcome of the analysis of a safety function. Findings are further categorized as critical, opportunity for improvement, and good practice. Critical findings represent significant vulnerability to system failure, similar to the July 2013 event. Opportunities for Improvement represent non-critical items for consideration under the continuous improvement process. Good practice findings are recognition of exemplary notable practices.

The facilitator recommended a modified Hazard and Operability (HAZOP) study process in lieu of a Failure Modes and Effects Analysis (FMEA.) A modified HAZOP is more comprehensive in that it evaluates failures due to deviations in not only equipment, but also controls such as administrative procedures.

2 Acronyms

1oo1 – 1 Out of 1 evaluation
AC – Alternating Current
AND – Logic function AND (TRUE if all inputs are TRUE)
DC – Direct Current
DH-13 – Dipole Horizontal magnet #13 PPS/TPS credited control to prevent beam transport to the Target.
DTL – Drift Tube LINAC (Linear Accelerator)
FE – Front-End
FSAD – Facility Safety Assessment Document
HAZOPS – Hazard and Operability Study
IPPS – Instrument Personnel Protection System
Linac – Linear Accelerator
MEBT – Medium Energy Beam Transport
MPS – Machine Protection System
N_2 – Nitrogen
NC – Normally Closed (Electrical Contact)
NO – Normally Open (Electrical Contact)
P&ID – Piping & Instrumentation Diagram
PPS – Personnel Protection System
RF – Radio Frequency
SRS – Safety Requirements Specification
SSRS – Safety Software Requirements Specification
TPPS – Target area Personnel Protection System
TPS – Target Protection System
XOR – Logic function Exclusive OR (TRUE if Only One Input TRUE)

3 Summary of Findings and Recommendations

The team concluded there were no critical findings, two good practice items, and seven opportunities for improvement. During the HAZOPS process, the team also noted areas not directly related to the scope of this study but important for further consideration. The remainder of this section summarizes the study results. See Section 6 for a detailed explanation and recommendation for each finding.

3.1 Good Practice

a.) SNS has made significant progress in validating and updating PPS documentation. This, in turn, made the HAZOP process easier to complete.

b.) The HAZOP process of identifying functional relationships between systems, hardware, and software was a good tool to update the institutional memory on why and how certain systems are configured the way they are. This, in turn, contributes to the long-term sustainability of PPS systems.

3.2 Critical Findings (None)

The HAZOP Team did not uncover new common mode failures.

3.3 Opportunities for Improvement

a.) The long-term corrective action to separate PPS power supply commons remains the best way to eliminate the previously identified common mode failure. [Section 6.3.1]

b.) Verify and consolidate information for the TPPS reach-back timers used to initiate back-up and emergency shutdown mechanisms should the primary methods fail. Incorrect specifications for these timers can prolong the PPS reaction to fault events. [Section 6.3.2]

c.) Review the reliance on trapped key systems as de-facto logic elements. Trapped key systems are effectively used as mechanical AND/XOR logic elements with limited status feedback. Top-level logic summaries infer the status of lower level trapped key logic. The Front End Plug Door trapped key system relies explicitly on a trapped key without direct PPS monitoring of the status of the movable shielding. [Sections 6.3.3 and 6.3.4]

d.) Review the PPS architectures where some permits are provided by only one PPS chain while the status of the final device is monitored redundantly. [Section 6.3.5]

e.) Evaluate the cost/benefit to minimize the variations in Instrument PPS (IPPS) equipment and architectures. The variability of the present beamlines, controls, and equipment open vulnerabilities to human error and sustainability issues. [Section 6.3.6]

f.) Review the DH13 TPS/PPS DC Disconnect system design with the goal of eliminating unsafe failure modes. Unsafe failure modes include ambiguous PPS status readback during a power failure and damage due to out of sequence control of the AC/DC power and the DC Disconnect. *Note: In addition to the DC disconnect, an AC Contactor and power supply controls provide redundant shutdown of DH13.* [Section 6.3.7]

g.) Mark or label mechanically similar devices like the DTL waveguide blanking plates to avoid installation errors. [Section 6.3.8]

4 Scope of this report

This report covers the HAZOPS for the Accelerator, Target, and Instrument PPS systems at the functional level. This includes interdependencies between systems, physical and functional redundancy. The primary scope is limited to identifying vulnerabilities that can directly contribute to failure of redundant systems as required by the corrective action. By its nature, a study of a system at the functional level includes systemic errors such as requirements and human error. The HAZOP Team also looked into elements or functions that do not require redundancy.

Limitations on time precluded in-depth analysis of all circuits, software, and processes. Rather, during the analysis process, the team identified areas for detailed analysis then drilled-down in sufficient detail to evaluate possible vulnerabilities.

This report assumes the reader is familiar with SNS operations, systems, nomenclature, and PPS functions. For a detailed description of the facility and PPS functions, see the Safety Assessment Documents for SNS Proton (PSAD) and Neutron (NSAD) Facilities [1] [2].

5 Methodology

The team used a modified Hazard and Operability (HAZOP) study process to evaluate the PPS. HAZOPs were originally developed as a means to review process control systems. Since its inception, HAZOPs have been adapted for use in several areas, notably software based systems [3] [4].

5.1 PPS HAZOP Team:

In a HAZOP, a team reviews a functional representation of a system or process' nominal operation, and then methodically evaluates the impact of deviations from the nominal operation. The team members were selected based on their knowledge of the systems and equipment under review. The process was facilitated by a PPS expert from Jefferson Lab experienced in the modified HAZOP process. The acting Protection Systems Team Leader served as the SNS HAZOP team leader. In addition to the core team, systems experts for non-PPS systems such as the Target Protection System (TPS) were consulted to validate the information used in the analysis.

Team Members

- Doug Curry, ORNL/SNS Acting Protection System Team Leader (SNS Lead)
- Kelly Mahoney, Jefferson Lab Safety Systems Engineering Manager (Facilitator)
- Aaron Coleman, ORNL/SNS Protection System Team Engineer
- Bryan Moss, ORNL/SNS Protection System Team Technician
- Melanie Smith, ORNL/SNS Protection System Team Technician
- Bill Stone, ORNL/SNS Protection System Team Engineer
- Derrick Williams, ORNL/SNS Process Controls Team Engineer

In this study, the team created functional models centered on PPS operational modes and the methods and credited controls used to establish safe operations. Models typically include multiple PPS segments and devices with the Front End as the ultimate termination point. Systems other than the PPS, such as TPS and MPS, are included in the models when they contribute to the completeness of a functional model.

5.2 Guidewords

Guidewords for this study are given in Table 1. HAZOPs use guidewords to describe deviations from the intended function. For example, "*redundantly detect and act to mitigate an access control violation*" is a function performed by the PPS. Deviations from the intended function may include *not detected, detected too late, mitigation too late, mitigation partially performed*.

The team evaluated deviations in the intended functional elements to determine potential failure mechanisms. Unless noted otherwise, the functional diagrams assume the PPS is fully redundant and therefore identified failure modes are common mode failures. The team noted functional elements that are implemented in only one PPS chain, such as primary shutter control, and then evaluated the impact to the overall redundant PPS system. In this case, the shutter position is sensed redundantly and both PPS chains can shut down the Front End if required.

5.3 Reviewed Documentation

In a HAZOP, as-built documentation is used as the primary information source for the study [5]. In this case, 'as-built' includes not only electrical and mechanical diagrams, but also PLC programs, specifications, procedures, and photographs. The team assembled and augmented this documentation as necessary to validate functions and equipment under review. Assumptions and clarifications were sustained by documentation.

The team worked primarily from the following documentation:

- Systems Requirements Specifications (SRS)
- Safety Software Requirements Specifications (SSRS)
- PPS PLC programs
- Wiring Diagrams
- Operations and Maintenance procedures
- Equipment and Component data sheets
- Test and Certification Documents
- Photographs of field installations

Table 1 - Guide Words

Guide Words	Meaning	Example	Alternate/Related Words
No, Not	Absence of; Negation of Intended Action	No Insert Command to Secondary Stopper; FE does not receive shutdown command	Failed
More	Parameter greater than intended	MEBT Stopper N_2 pressure more than component rating	Greater than, Over
Less	Parameter below intended	Command to close primary shutter less than minimum 50ms	Less than, below, under
As Well As	Intended Action plus unintended action occurs	65kV as well as plasma RF enabled in open access	Also, AND, too
Reverse	Opposite action; order; condition	The Primary Beam Stop NO and NC PPS switch read backs are reversed	Switched, Opposite
Other Than	Action excludes intended actions	Trapped Key removed in state other than intended	Except
Early	Action occurs before intended timing	Shutdown to FE occurs early	Too soon
Late	Action occurs after intended timing	Reach-back to FE shutdown occurs late	Too late
Partially	Incomplete action or condition	Horizontal secondary shutter partially inserted	Incomplete
Before	Action precedes intended sequence	Ion Source turns ON before Beam Permit delay timer complete	Previous to
After	Action is post intended sequence	Secondary shutter closes after fault timer complete	Following

6 Findings

6.1 Noted Good Practice

a.) Team members were exceptionally knowledgeable about the broad spectrum of PPS systems and equipment.

b.) SNS has made significant progress in validating and updating PPS documentation. This, in turn, allowed the HAZOP team to assure the accuracy and validity of supporting documentation. SNS will continue to benefit from this effort.

c.) The HAZOPS process enabled the team to gather and document interdependencies between multiple PPS systems and equipment. Much of this information was formerly institutional knowledge. Documenting the system level function and design basis for many of the protection systems increases sustainability of current SNS operations as well as enhances the design basis for future projects such as the Second Target Station.

6.2 Critical Findings (None)

There were no critical findings of functional failures of the PPS.

6.3 Opportunities for Improvement

During the HAZOP process, the team identified several opportunities for improvement to make the PPS more robust, reliable, and well documented.

6.3.1 Power Supply Grounding

The team did not identify failure modes similar to the July 2013 grounding issue, which was addressed during the winter 2014 shutdown. Although the modifications are effective, no latent common failure modes other than the grounding issue previously described were discovered. There is potential for common mode failures on some instrument systems, however, unlike the accelerator intersegment communication problem, these systems will fail-safe. The long-term improvement project to separate PPS commons remains a high priority.

Recommendation:
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.

6.3.2 TPPS Reach-back (X, Y, Z) Timers

The Target PPS uses three timers, X, Y, Z, to monitor the time for a primary safety function, e.g. "*Insert Secondary Shutter when there is an IPPS Fault*", to transition before reaching back to the next upstream function, e.g. "*insert primary shutter*", if the secondary should fail to close. These timers represent the maximum acceptable time for the Secondary Shutter to close, the Primary Shutter to close, and the time for the Primary Shutter to transition off of its open limit switch respectively prior to engaging additional protective measures upstream of the TPPS and IPPS.
Cumulative timer values range between minutes for low hazard beam lines to zero for high hazard beam lines. The required timer values are extracted from the Neutronics Study results for each beamline and may be different for primary

and secondary IPPS faults. The TPPS X, Y, Z timers for each beam line create a vulnerability to personnel exposure to radiation if the timer values are incorrect; e.g. if the time to react to a beam line 3 fault was set to 120 seconds as opposed to 0 seconds. Similarly, values shorter than the required value could lead to spurious trips affecting all instrument lines.

The TPPS Software Safety Requirements Specification [6] describes the function of the X, Y, Z timers but defers the specific values for each instrument line to the respective Instrument SSRS. At least some of the Instrument SSRS' [7] [8] differ from the TPPS SSRS in the description of the function and initiating logic for the X, Y, Z timers. The function of the Y and Z timers are reversed between the IPPS and TPPS documents.
The TPPS SSRS statement "Generally, the Y timer will always be set to zero for an IPPS Fault condition" is not reflected in the IPPS software specifications. Note: the statement appears to be true for the IPPS 'X' timers. The TPPS PLC software reviewed by the Team did not use the terms 'X','Y', and 'Z' in the tag names of the timers [9].
These discrepancies, coupled with other human factors, could lead to a functional failure if the SSRS gives an incorrect value for the X, Y, Z timers or the value is misinterpreted by TPPS programmers. There is no evidence at this time that such an error has occurred.

Recommendations:

a.) Verify the values for the TPPS X, Y, Z Access 01, Access 02, and Fault timers are correctly specified in each Instrument SSRS.
b.) Verify the TPPS/IPPS certification procedures validate the X, Y, Z timers documented in the current IPPS SSRSs.
c.) If possible, verify the TPPS PLC Program values of the X, Y, Z timers for each active instrument beam line.
d.) Revise the TPPS SSRS, IPPS SSRS' and TPPS program tags to eliminate ambiguity and generalizations. *Note: PLC tags are text-based aliases for physical memory locations in the PLC. They exist in a database outside of the PLC program and have no effect of the execution of PLC logic programs.*

6.3.3 Reliance on trapped key logic

Trapped exchange keys are used throughout the SNS PPS systems. In many instances, master keys represent the logical summation of several sub-functions. In an extreme case, the Target key bank exchanges keys with over 10 panels and sub panels controlling critical devices, access controls, machine modes, and shielding (See [10]). Most of the sub-function keys are not monitored; the PPS safety functions partly rely on the mechanical integrity of the key banks to infer a monitored key reflects the underlying logic. While it is standard practice at other Labs to use exchange keys in simple AND/XOR logic, some of the functions at SNS are complex. With the exception of the Front End Plug Door, the safety functions incorporating trapped keys and evaluated by the HAZOP Team were backed up by PPS monitoring of devices required to establish a safe machine configuration. For example, if the Front End master key (Fi) were removed and inserted in the Front End Only key panel, the monitored status of the DTL waveguide and MEBT stop credited controls would prevent Front End Only beam operation.

Recommendation:
Conduct a more in-depth review of the trapped key logic along with associated operating procedures and PPS logic to verify PPS safety functions are not compromised if there is a logical failure of a mechanical component. This should also verify PPS functions are not bypassed based solely on the status of a trapped key configuration.

6.3.4 Plug Door Trapped Key

The configuration of the Front End Plug Door is not directly monitored by the PPS. The plug door is held in place using two administrative controls: A radiation safety lock and a trapped key (Fg) securing a chain connecting the trapped key unit to the plug wall. The Fg key and chain are normally removed using the Fb key which disables LINAC operational modes. Failure of the integrity of the Fg trapped key mechanism could allow the plug door to be opened without tripping the PPS. The hazard under consideration is personnel access to the LINAC section during beam and RF operations. Good practice for accelerator facilities recommends movable shielding be locked and interlocked.

Recommendation:
Investigate the cost/benefits of adding redundant LINAC PPS interlocks to the plug door.

6.3.5 Position Switches as Credited Controls

The reliance on position switches as 'credited controls' requires further study. Extending from this philosophy is justification for single chain permits to protection devices like shutters and stoppers. A control is the thing that acts to mitigate an identified hazard. In the case of the target and instrument lines, this means that the only fully redundant credited controls for instrument operation are the DH13 and front-end shutdown mechanisms.
The reach-back functions such as those performed by the Target PPS are essentially stand-by functional redundancy with single chain (1oo1) shutdown capability. This architecture may be completely satisfactory given the relatively low hazards in the Instrument beam lines. However, the reliability of this approach should be revisited in the context of this report.

Recommendation:
Use appropriate reliability models to determine the safety/availability impact of single-permit/redundant-monitoring architecture.

6.3.6 Multiple Instrument Beam Line PPS Architectures

There are multiple PPS architectures for instrument beam lines developed as standards and methods evolved over the SNS project. The present system opens the door for systematic human error based on having to know exceptions/nuisances of each beamline.
Note: This includes not only PPS devices but also ancillary devices such as secondary shutters and shutter controls. Variability among devices like the secondary shutters and associated controls complicates the ability to assure required reliability, failure modes, and configuration control.

Recommendations:

a.) Evaluate the feasibility of consolidating instrument beam line PPS architectures into a few well-documented approaches.

b.) Evaluate the feasibility of consolidating the types of instrument beam line secondary shutters and controls.

6.3.7 DH13 PPS/TPS Control

Power failure to the DH13 DC Disconnect controls will de-energize the PPS status readback relay PPS-A2. The relay fails UNSAFE in that the zero power state indicates to the PPS the DC disconnect is OFF (Dump Position) even if the disconnect is ON (Target Station Position) [11].

The DH13 controls require the DC current to be removed before the DC Disconnect Switch changes state. Failure to do so could damage the disconnect contacts. The failure mode of DC Disconnect contacts welded closed AND the power to relay PPS-A2 OFF (Failed UNSAFE) was considered as an unlikely but credible failure mode. The AC Contactor controls and Power Supply Control interface (System A Only) provide sufficient redundancy between inspection and certification intervals.

Recommendation:

Review the DC Disconnect system design with the goal of eliminating unsafe failure modes.

6.3.8 DTL Waveguide Short Installation

The Waveguide shorts installed on DTL waveguides DTL-1 and DTL-2 for Front End Only mode can be installed on the opposite waveguide (reversed). The position switches are coded and should fail-safe. This situation could result in unnecessary down time.

Recommendation:

Mark the waveguide shorts and associated waveguides to reduce the likelihood of reversed installation.

6.4 Additional Items for Consideration:

In addition to the findings, above, the PPS HAZOP Team generated following additional items for consideration for future evaluation.

6.4.1 Primary Shutter Controls

Perform a HAZOP of the Primary Shutter control systems. This would follow a more traditional HAZOP process using P&ID drawings. One area for consideration is the performance of the primary shutter hydraulic systems when commanded to simultaneously drive all shutters to the closed position.

6.4.2 Configuration management of PPS control panel keys

Some of the control keys (not trapped keys) used in IPPS panels are standard-off-the shelf items readily available from manufacturer stock. The PST should evaluate vulnerabilities associated with readily available and interchangeable key controls. The PST should further evaluate the uniqueness of the trapped keys.

6.4.3 Independent verification of System A and B Indicators

Existing certification procedures challenge the integrity of both A and B simultaneously but not independently. This limits the ability to identify single failures, i.e. interface relays that are used to energize or de-energize power supplies. The certification procedures should include steps that challenge these interfaces separately.

6.4.4 RS Holds on Trap Keys

Alternate methods or additional steps should be taken into consideration when applying RS-Holds to Trap Keys, i.e. "U-keys" for the Primary Shutter. Trap keys are not unique and replacement keys can be purchased from the vendor. It is possible, however unlikely, that a duplicate key could be installed and used to operate a device that has an RS-Hold applied to the original Trap Key.

7 Conclusion

This report documents the systematic evaluation of PPS functions and equipment with the intent to uncover latent systematic or common failure modes. No method is 100% effective, however this effort significantly contributed to re-establishing confidence in the basic PPS design and architecture. Although no new common mode failures were identified, the HAZOP Team did identify several vulnerabilities that could contribute to systematic failures under certain circumstances. Future actions should consolidate and prioritize the recommendations of this report with those identified in previous reviews and reports. Elimination of the previously identified common ground failure mode should remain the highest priority among the recommendations. SNS management should incorporate baseline PPS improvements in their long range goals and plans.

8 References

[1] OAK RIDGE NATIONAL LABORATORY, *Spallation Neutron Source Facility Safety Assessment Document Protron Facilities,* Oak Ridge, TN, 2010.

[2] OAK RIDGE NATIONAL LABORATORY, *Spallation Neutron Source Final Safety Assessment Document forNeutron Facilities,* Oak Ridge, TN, 2011.

[3] F. Redmill, M. Chudleigh and J. Catmur, Systems Safety: Hazop and Software Hazop, New York: Wiley, 1999.

[4] N. G. Leveson, Safeware: System Safety and Computing, New York: Addison-Wesley Professional, 1995.

[5] N. J. Bahr, System Safety Engineering and Risk Assessment: A Practical Approach, New York: Taylor and Francis, 1997.

[6] PST, *Target PPS Software Safety Requirements Specification,* 2013.

[7] PST, *IPPS Software Safety Requirements Specification: Neutron Spin Echo Spectrometer [BL15],* 2011.

[8] PST, *IPPS Software Safety Requirements Specification: Single Crystal Diffractometer [TOPAZ] [BL12],* 2009.

[9] PST, *PPS Target PLC Program System A Rev02,* 2012.

[10] PST, *PPS CCR Key Exchange Drawing,* 2006.

[11] TPS Engineering, *SNS-OPM 7.T-16 (Y) TPS Test Procedure.*