SNS PPS Consulting Report November 18-22, 2013 K. Mahoney
Revision – December 30, 2013

Under work conducted under management purchase order 0505429, Kelly Mahoney of Jefferson Lab is tasked with assisting in the evaluation and implementation of corrective actions related to the July 2013 PPS common mode failure event. This report documents the status of the work to date and recommendations based on interim findings.

Findings and recommendations

1. *Conduct an internal review of PPS system architecture and an associated Failure Modes and Effects Analysis (FMEA) to determine if other unanalyzed failure modes are possible. (ORPS-CHRIDGE-2013-0005, #7)*
   Reviewed the PPS architecture to the extent possible with the available documentation. There is documentation at the high level intended mostly for system overviews and external reviews. This documentation is an abstraction of the as-built system and is not intended to serve as a living document. The documentation of installed systems consists of wire lists in the form of spread sheets. This level of documentation is intended for installation and is not adequate to conduct engineering level reviews of architecture. A major effort of the last four month is to create engineering drawings of the as-built CCR PPS systems. This effort should continue in order to establish baseline documentation adequate to complete the intent of this corrective action.

   Although no failure mode was observed in the material reviewed to date, one apparent vulnerability for systematic errors is the failure to manage changes to system requirements.

   Further document the as-built architecture and review the number and control mechanisms for critical devices.

   The low level documentation is composed of spreadsheets serving as a wire list. Neither of these is adequate to serve the intent of this corrective action.
   a. Recommendation:
      i. SNS should commit to improving the hazard and failure mode analysis **process** as an integral part of the development, test, change, and operability lifecycle steps. It is more productive to improve the deficiencies in the process and apply the improved process.
      ii. Part of this action is to apply this process to existing designs as documentation is developed.
   b. This corrective action as stated is logically inconsistent and impossible to fulfill. I agree with the intent that SNS should systematically review the existing PPS implementations and management processes to look for additional unsafe failure modes.
   c. Without detailed drawings, an FMEA is not practical. Even at that, the process would not likely catch something like the July common mode failure. An FMEA would definitely not catch deficiencies in change and testing. It is equally likely an FMEA will not result in a common mode failure 'smoking gun'. Further, a system design should be robust against common mode and functional failures – e.g. single path shutdown commands.
   d. Develop system level block diagrams to aid in evaluation of the system architecture.
   e. A Hazard and Operability (HAZOP) or similar process is better suited to evaluate the potential for systems or personnel to deviate from the intended function.
   f. KM Presently looking at a representative field rack to see if the identified common mode failure is possible in other PPS installations.
      i. More time is required to develop sufficient documentation that accurately describes the architecture. Once this is done, a HAZOP may be more appropriate.
   g. Software review:

i. The System B software is now orphaned. As with the hardware documentation, the older software documentation is not well documented or sustainable.
ii. Many subroutines do not have a definitive return expression.
iii. System A Software:
    1. Missing or unused subroutines
        a. Although it is called by multiple fault traps in the main routine, the subroutine "Fault_Routine" contains only a NOP.
iv. System B software:
    1. System B software is written using a mix of Structured Text, Sequential Function Chart, and Ladder Diagrams.
        a. SNS should send personnel to advanced RSLogix software training to gain experience with the multiple programming languages.
        b. SNS should document the implementation of the System B software
        c. THEN and ONLY THEN SNS should consider converting the System B software to a more sustainable language as well as a language that is compatible with IEC61138 Safety extensions.

2. *Perform an in-depth review of adequacy of PPS procedures for configuration control, change requests, and testing/certification. (ORPS-CHRIDGE-2013-0005, #9)*
There is a comprehensive set of procedures for configuration control, change control, and testing. The procedures are readily accessible on-line to SNS personnel. However, much of this documentation needs to be scrubbed for relevancy and updated to reflect present work processes.
Access to the documentation is divided between the OPM system providing links to high level policies and procedures, and the ProjectWise system which contains all documentation including specifications, drawings, reports, and procedures.
SNS Procedures OPM 9.A.1 and 9.A.3 define the overall SNS configuration management process. Especially notable, procedure 9.A.3 SSCS Change Procedure includes a process map.
The PPS Team is revising a Credited Engineering Control (CEC) specific configuration management procedure (OPM 3.A-8.1) as a supplement to the overarching 9.A.1 and 9.A.3 documents.
The PPS Team uses student interns to write test procedures and perform QA on existing procedures. Recently, they have also been used to perform gap analysis of specifications and test procedures. The students have made positive contributions to the process management, to include documenting how the change process is implemented in the field. This type of information will be very useful in creation of process maps.

    a. SNS Configuration Management Policy 9.A-1 requires establishment of a "reference design configuration." This is a system baseline configuration as well as a list of elements under configuration management. At this time there is not a comprehensive list of PPS elements under configuration management.
        i. The PS Team Leader should develop a list of PPS elements under configuration management. This can start as a list of unique classes of elements such as door switches, stoppers, and RF controls sorted in to graded buckets. A more comprehensive list would include a full inventory of devices.

    b. The quality and consistency of the reviewed documentation roughly corresponds to the time it was developed with the Linac having the most problems and the target

instrumentation systems having the better documentation. Due to the aggressive operations schedule , demand to bring new instrument packages on-line, and limited qualified staff, the PS team has not been able to go back and update older documentation.

i. The PPS Team should make a concerted effort to bring all documentation up to date. This may be a multi-year project.
ii. Create a hierarchical list of PPS documents under configuration management showing the relationship between documents. Define an order of precedence between the documents.

c. Many procedures are orphaned, with the originator no longer at the Lab or no longer accepting responsibility for ownership. There is an issue with transfer of responsibility for certification procedures between the Operations Group and the RPS Team. A first principle implemented at SNS, as recommended by BNL, is to ensure an organization outside of the RPS group write the test procedures. However, Operations no longer accepts responsibility for writing PPS Certification Procedures.
    i. The PS Team Leader should immediately take ownership of certification procedures. If there are cross- department disagreements, have the RAD Head make final decision and officially assign responsibilities and expectations. David Freeman should be consulted as to the requirement for separation of personnel implementing the PPS and personnel performing acceptance testing.

d. The present PPS configuration management system has a major shortcoming in that the subject configuration management programs are not based on the systems requirements/specification documentation. This leaves a vulnerability that a change may inadvertently alter the intent of the system requirements. This also allows individual processes to diverge, increasing the likelihood of incomplete or inadequate design or testing. Inadequate requirements or deviation from requirements is one of the major root causes of common mode failures.
    i. Create a hierarchy of documents under configuration management.
    ii. Update all of the PS systems and software requirements documents for all PSS segments. The end result should be that the requirements/specifications are the governing documents against which all change proposals are evaluated.

e. Many procedures are effectively out of date. Recent attempts to update them do not address simple QA issues like dead links, obsolete references, …etc.
    i. Use the student intern help to go through all PPS procedures and forms to verify links and references are current.

f. The proposed update to the Configuration Management Procedure OPM 3.A-8.1 "Configuration Management Procedure for Credited Engineering Controls" requires substantial revisions for content and clarity.
    i. KM is revising document to be used as an example.

g. Certification procedures do not include a detailed list of items under test.
    i. Recommend that the Part I certification include a separate checklist that accounts for every PPS I/O point and device under test. The Test Director should sign off on this list as part of the Certification documentation.

h. The Service Bay Differential Pressure Monitoring system provides local evacuation alarms in the Target Building and an alarm in the CCR. However, we could not locate an operations procedure for what to do if the alarm annunciated in the

control room. Without guidance, A SBDPMS alarm response is subject to human error; as witnessed in the recent JPARC event, this can lead to unnecessary low level radiation exposures.

i. Need an Ops procedure for Target Bay Differential Pressure Alarm response or incorporate an existing procedure into the Ops emergency response section of the OPM system.

i. The procedure for Chipmunk removal requires the unit be tested before removal and after re-installation. However, there is no process for what to do if the unit fails the pre-removal test; i.e. it has been operation in a failed condition during operations.

i. In order to ensure a reasoned and rational response, SNS needs to pre-determine a process to follow if a Chipmunk fails pre-removal test.

j. Many PPS procedures and documents refer to "Phase 4.0" in the title. This refers to the original SNS incremental commissioning of machine segments.

i. Recommend "Phase 4.0" be removed from the PPS documentation. This term is obsolete and confusing when used in the same context as Phase I and Phase II PPS testing.

k. While the OPM web access links to the latest revision of a document, the ProjectWise database shows all revision in a flat list. It is very difficult to ensure one is accessing the latest revision of a document from ProjectWise.

i. Investigate the utility of using existing ProjectWise features that allow storage and retrieval based on revision levels.

l. The Chipmunk design is essentially orphaned and not supported in-house.

i. KM will look at Chipmunk design.

m. Recommend KM work with PPS/SNS staff to develop process maps for the PPS lifecycle including design, change, configuration control, and testing.

n. KM provide an outline of procedures with suggested content. Suggested content includes clear roles, responsibilities, and authority; references; scope;

3. *Conduct external reviews of FMEA and system architecture analysis results. (ORPS-CHRIDGE-2013-0005, #8)*

4. *Implement any necessary changes to PPS systems and procedures that result from Corrective Actions 7-9. (ORPS-CHRIDGE-2013-0005, #10)*

Short Term solution under way. PS engineering not sure if part 2 can be accomplished in July 2014. Both the short and long term fixes need a task and key deliverable based schedule – Who is doing what when? SNS management must approve the final schedule and ensure priorities are clearly communicated. If a deliverable is delayed, it must be justified and approved.

5. Other Observations:
   a. Personnel
      i. The Protection System Team staffing is insufficient to carry out its mission given the present work load, management processes, and skill mix. Presently, the core group is composed of three nuclear engineers – including the Team Leader - and two technicians, one of whom is dedicated to Chipmunk support. The team is presently augmented with the assistance of a controls engineer and a contract designer.
         1. Recommendations:

a. Add an experienced electrical/industrial controls engineer to the team. This person should have experience or be trained in safety systems.
b. Add one electrical/electronics technician to the team for general PPS development and support.
c. Add at least one dedicated designer for baseline documentation support; an additional designer may be required through September 2014 to get drawings to a sustainable level.
d. At least one of the student interns should be an electrical/industrial engineer (as opposed to nuclear).
e. The Data Systems Department should have a technical writer/editor with priority given to managing and improving protection systems documentation.