OAK RIDGE National Laboratory

PO Box 2008
Oak Ridge, TN 37831-6250
(865) 574-9113 |webbrc@ornl.gov

Date: October 31, 2014

To: J. W. Smith, M.L. Baker, R.A. Crone, and K.W. Jones

c/att: Distribution

From: R. C. Webb

Subject: **IO-2014-2 SNS Configuration Management Review of Credited Engineered Controls**

Independent Oversight conducted a review of the SNS Configuration Management (CM), specifically to evaluate the configuration management-related actions completed in response to the ORPS event SC-ORO--ORNL-X10CHRIDGE-2013-0005 - Discovery of Non-Operable Safety System during Testing. Additionally, five Credited Engineered Control (CEC) systems were identified for review of configuration management by the Review Team.

If you have any questions, please contact Edward Lessard, Assessment Team Leader, at 631-344-4250 or me at 865-574-9113.

Attachment – IO-2014-2 SNS Configuration Management Review of Credited Engineered Controls Assessment Report

ORNL Management and Staff:

M. L. Baker
K. A. Carney
R.A. Crone
S. S. Davis
M. B. Farrar
V. S. Fowler
D. L. Jenkins
K. B. Jeskie
P. G. Johnson
K.W. Jones
S. C. Kohler
C. G. Lewis
D. J. Mandl
C. H. Scott
J. W. Smith
B. J. Verastegui
R. C. Webb

Department of Energy:

D.K. Arakawa, DOE-OSO
M. G. Branton, DOE-OSO
D. M. Carden, DOE-OSO
D.M. Hoag, DOE-OSO
M. J. Kass, DOE-OSO
J. O. Moore, DOE-OSO
D.E. Paul, DOE-OSO

Battelle Corporate and Affiliates:

J. Alvarez, Idaho National Laboratory
J.L. Mobley, Battelle

Assessment Team:

Ed Lessard, BNL – Team Lead
Enzo Carrone, SLAC
John Forrestal, ANL
Natasha Blair, ORNL
John Young, DOE- OSO
Kyle Turner, Mc-Callum-Turner, Inc.

OAK RIDGE
NATIONAL LABORATORY
MANAGED BY UT-BATTELLE
FOR THE DEPARTMENT OF ENERGY

Independent Oversight

SNS Configuration Management Review of Credited Engineered Controls

IO-2014-2
October 2014

UT-BATTELLE

ORNL-27 (4-00)

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE, LLC, FOR THE DEPARTMENT OF ENERGY

SNS Configuration Management Review of Credited Engineered Controls

PROJECT NUMBER
IO-2014-2

Submitted by:

Edward T Lessard

Edward Lessard
Assessment Team Leader

Approved by:

Rebecca C. Webb

Rebecca Webb
Independent Oversight Leader

SNS Configuration Management of Credited Engineered Controls

Table of Contents

EXECUTIVE SUMMARY 1
SCOPE AND METHODOLOGY 4
ASSESSMENT RESULTS 5
ASSESSMENT CONCLUSIONS 10
APPENDIX A - ASSESSOR BIOGRAPHICAL INFORMATION 11
APPENDIX B - STAFF INTERVIEWED 14
APPENDIX C - DOCUMENTS REVIEWED 15

ABBREVIATIONS, ACRONYMS, AND INITIALISMS

ACTS	Action Commitment Tracking System
ANL	Argonne National Laboratory
AR	Assessment Results
ASE	Accelerator Safety Envelope
BNL	Brookhaven National Laboratory
CCC	Configuration Control Committee
CEC	Credited Engineered Controls
CM	Configuration Management
DOE	Department of Energy
IO	Independent Oversight
IOP	Internal Operating Procedure
IPPS	Instrument Personnel Protection System
NScD	Neutron Sciences Directorate
ODHSIS	Oxygen Deficiency hazard Safety Instrumented System
OPM	Operations Procedures Manual
ORNL	Oak Ridge National Laboratory
ORPS	Occurrence Reporting and Processing System
PPS	Personnel Protection System
R2A2	Roles, Responsibilities, Authorities, and Accountabilities
R&D	Research and Development
RAD	Research Accelerator Division
SAD	Safety Accelerator Design
SBMS	Standards Based Management System
SLAC	Stanford Linear Accelerator Center
SME	Subject Matter Expert
SNS	Spallation Neutron Source
TBAC	Transfer Bay Access Control System
TPS	Target Protection System

EXECUTIVE SUMMARY

BACKGROUND AND OBJECTIVES

On July 31, 2013, Instrument Personnel Protection System (IPPS) certification testing at the Spallation Neutron Source (SNS) revealed a failure of the Personnel Protection System (PPS) that prevented PPS system operability as required. The PPS/IPPS systems are Credited Engineered Controls (CEC) that prevent entry into areas with significant radiation hazard, trip the accelerator beam off when specific radiation levels are detected in areas that may be occupied, and prohibit beam to the target when the target cart is not inserted. Additional PPS safety functions are listed in the SNS SADs. The approved Accelerator Safety Envelope (ASE) specifies that the PPS shall be operable to support the applicable operational configuration during operations with beam. Prior to starting the IPPS certification, limited beam operation had been initiated to support the transition from maintenance to beam operations. This event was reported into ORPS under SC-ORO--ORNL-X10CHRIDGE-2013-0005 - Discovery of Non-Operable Safety System during Testing.

Among the corrective actions implemented in response to the ORPS event (ACTS .28733) were actions to enhance the effectiveness of the SNS configuration management process for safety systems. To provide a robust independent review of the overall effectiveness of these enhanced processes at SNS, the ORNL IO office was commissioned to conduct a review of configuration management of safety systems at SNS.

RESULTS

The team determined SNS management understood the importance of configuration management and that it was understood and accepted by SNS staff. There was clear evidence that configuration management procedures are being implemented. Corrective actions completed in response to the ORPS event were effective in improving the CM process. There was good evidence of physical CM of CECs (labeling and access). The Configuration Control Committee (CCC) was active. There was management commitment to improving CM processes, which was demonstrated by the existence of a "NScD Operational Quality and Efficiency Improvement Plan."

Ten specific CM related areas involving SNS operations were assessed by reviewing documents and interviewing System Engineers, Committee Chairs, SNS Managers, Group Leaders, Protection System Group staff and others. Specific results are documented in the Assessments Results section for the following:

1. Document Control
2. Configuration Management of CECs: Procedures 3.A-8.1 and 3.A-8.2
3. Configuration Management Procedure 9.A Series
4. General Operating Procedures in OPM
5. Configuration Control Committee
6. Training
7. Independent Review

8. Contractor Assurance
9. CEC Requirements Document
10. R2A2s

Recommendations: Based on the Assessment Results (AR), the Team developed the following recommendations to improve effectiveness of CM for CECs:

1. CEC drawings should be readily retrievable and current (See AR 1)
2. Test plans for CEC modifications should be controlled documents (See AR 1)
3. An update to the 3.A-8 series procedures is needed to ensure 1) consistency between records and the narrative in the procedures, 2) level 1 and level 2 modifications are fully defined, and 3) temporary changes provide the same level of protection as permanent changes (See AR 2)
4. The significance and use of signatures on CEC related records following a change needs clarification (e.g., technical review, approval of post-change testing, approval to operate post change, QA or QC review, CCC review of the change was completed) (See ARs 1, 2, 4, 5)
5. OPM procedures that may not exist in the OPM but may be useful would include Delegation of Authority, Acceptance Testing and Storage of CEC Parts, and Version Control for Software and Firmware on PLCs Used in CECs (See AR 4)
6. The CCC should consider 1) adding the Safety Documentation Manager and other technical specialists to the committee, 2) providing a list of all the reviews required for a specific CEC change, and 3) performing field visits before and after a CEC modification (See AR 5)
7. Safety basis training should be given to System Engineers, QA/QC staff, CCC members, Protection Systems Group staff and others who interface with CECs (See AR 6)
8. Robust independent review should be fully implemented for proposed CEC design changes, for proposed CEC testing procedures and for review of CEC test results post change (See AR 7)
9. Contractor assurance processes should be clearly defined for OPM procedure modifications or for CEC modifications and post-change testing. Contractor assurance processes should be integrated into the CCC, OPM and CEC processes and include steps to identify deficiencies and opportunities for improvement, report deficiencies to the responsible manager, complete corrective actions and report lessons learned effectively across all aspects of SNS operation) (See AR 8)
10. A CEC requirements-document for in-house protection systems should be developed and finalized (See AR 9)
11. R2A2s should be controlled and a special R2A2 for a System Engineer assigned to a CEC is suggested (See AR 10)

The Team developed the following recommendations to improve overall performance:

1. The drawing update initiative should continue and priority given on a risk based approach and planned modification schedule (See AR 1)
2. Increased rigor is needed for committee charters, R2A2s, ACL travelers, and configuration control of CCC records (See AR 1)

3. An update to the 9.A series procedures is needed to ensure 1) the USI process matches USI screening methods used in practice, 2) the Configuration Control Committee (CCC) process description is emphasized, and 3) guidance on when a CCC review is required is stronger and clearer (See AR 3)
4. Updates and periodic reviews of all procedures in the OPM should be performed in order to maintain them administratively and technically current (See AR 4)
5. System Engineers and staff who implement modifications should be trained in the CCC process (See AR 6)
6. The identification of training requirements and implementation of training for new or revised OPM procedures should be performed (See AR 6)

SCOPE AND METHODOLOGY

IO conducted a review of the SNS Configuration Management of Credited Engineered Controlled Systems in September 2014.

ASSESSMENT OBJECTIVES

The objective of the review was to evaluate the configuration management-related actions completed in response to the ORPS event SC-ORO--ORNL-X10CHRIDGE-2013-0005 - Discovery of Non-Operable Safety System during Testing. Additionally, five Credited Engineered Control systems were identified for review of configuration management by the Review Team.

The overall approach to this assessment was to review effectiveness of implementation of the following procedures of the SNS Operations Procedure Manual – Section 3:

- 3.A-8.1, Configuration Management Procedure for the following Credited Engineering Controls: PPS, TBAC, SBDPMS and TPS
- 3.A-8.2, Control of Temporary Hardware Changes/Bypasses: Personnel Protection System (PPS), Transfer Bay Access Control (TBAC), Service Bay Differential Pressure Monitoring System (SBDPMS) and Target Protection System (TPS)

Scope of the review included procedures for conformance with applicable provisions of Contractor Requirements Document in DOE Order 420.2C, *Safety of Accelerator Facilities*, as well as implementation of the SNS procedures for the PPS system. Configuration management-related actions completed in response to the ORPS event described above were also examined. Additionally, a total of 5 CECs (see SNS Credited Engineered Controls List, 102030100-ES00007-R01) were identified for a review of configuration management by the Review Team.

- Target Protection System (TPS)
  - Cuts off the proton beam when necessary to prevent overheating of mercury due to inadequate mercury loop flow or cooling
  - Prevents beam on target when target when target carriage withdrawn
- Transfer Bay Access Control System
  - Protects worker from excessive radiation and/or airborne Hg by preventing access to transfer bay when with the upper or lower segment of the intra-bay shielding door is not closed. Sounds an alarm if intra-bay door segment becomes not closed during access.
- Target and Instrument PPS
  - Target PPS – Prevent potentially injurious exposure to prompt radiation [by the target cart position interlock and by executing protective response to Instrument PPS fault signal(s).]
  - Instrument PPS – In general, all instrument enclosures: Prevents potentially injurious radiation exposure to prompt radiation in instrument enclosures.
  - Instrument PPS – Specific instrument enclosures: Monitor O_2 concentration and provide alarm in the event of inert gas release inside an enclosure.

- Personnel Protection System (PPS)
    - Prevent potentially injurious radiation exposure to prompt accelerator radiation.
- Oxygen Deficiency Hazard Safety Instrumented System
    - Monitors oxygen levels in the superconducting LINAC (SCL) and the CHL and provides visible and audible alarms inside the areas and at entrances when the decreased oxygen level indicates a significant release of inert gas may have occurred from the cryogenic system.

ASSESSMENT RESULTS

1. Document Control
    1.1. CEC drawings need to be readily retrievable and current, as a platform for work planning, as well as to ensure that configuration control of CEC systems is effective. Accordingly, the drawing update initiative currently in process at SNS should continue. Priority for individual drawing updates should be assigned using a risk-based approach (highest hazard systems first) and in consideration of planned CEC modification schedules (so that drawings for CECs planned for near-term modifications would be at the top of the update queue).
    1.2. More rigor is needed in committee charters (e.g., CCC, RSC, ISSC, CSC, ESC), ACL travelers, and configuration control committee records to foster consistency and ensure that committee decisions and the associated rationale are appropriately documented.
    1.3. Test plans for CEC post-modification testing need to be treated as controlled documents to ensure that tests demonstrate that modifications maintain CEC functionality and that the annual certification tests are updated, as applicable, to reflect post-modification configuration and functionality.
    1.4. The ACL traveler and associated acceptance list should be elevated to the status of a controlled document. Also, the functional role of the QAR should be clearly delineated (with QAR training and qualification requirements established as appropriate to this role; see AR 6) and the originating document (e.g., procedure, policy) that codifies use of the ACL traveler clearly identified.

2. Configuration Management of CECs: Procedures 3.A-8.1 and 3.A-8.2
    2.1. These procedures would benefit from charting the flow of steps, recording the results in a flowchart to be incorporated into the procedures, and updating procedures accordingly. As a part of procedure updates:
        2.1.1. Ensure consistency between and within records and the narrative description of steps in the processes.
        2.1.2. Provide more definition on the types of activities that would constitute Level 1 and Level 2 modifications.
        2.1.3. Clarify the meaning of signatures on Form 3.A.8.1a, so that the context of their input to the procedural process is clear; in the procedure text, ensure the role of signatories (e.g., authorization, approval, concurrence, recognition of notification) is clearly defined.

2.1.4. Clarify whether signatures of committee chairs connote their individual roles or a resolution from the committee they chair.

2.2. Consider including temporary changes in 3.A-8.1 (versus under 3.A-8.2, as currently configured) to ensure that the same level of protection of CEC functionality is maintained, regardless of how the modification is characterized. (The Team notes that impacts on CEC functionality can be as great for temporary modifications as for non-temporary ones.) If restructured in this fashion, 3.A-8.2 would be specific to bypass activities only.

2.3. There is a gray area between 3.A-8.1 and 3.A-8.2 concerning maintenance activities on components that are not being modified, only removed for maintenance with the expectation they will be returned to service before beam operations can resume. The former is a modification to the system that will support operations and thus comes under Level 1. The latter requires thorough testing ensuring it operates as specified. This distinction should be made in 3.A-8.2, including "like for like" replacements where failed components are being replaced or substituted with newer hardware.

2.4. Within the Level 1 process, address the differences between significant changes to the PPS or minor modifications that do not affect safety functionality. This distinction could be made with concurrence of the Safety System Engineer, Team Leader, USI screener and CCC chair.

2.4.1. This process should be identified on the flow chart.

2.4.2. Verification that no un-intended changes are made would be determined by re-certification of the affected system including final "End to End" tests.

2.4.3. Verification the CEC operates as intended after hardware changes can be made by through testing of affected devices (e.g. module replacement requires verification all I/O functions execute as designed). "End to End" testing should be included in this process.

2.5. Meeting the requirements of Section 5.4.4 of SMS-OPM 3.A-8.1.a (Rev 06) should be addressed on a per case basis, for example requiring a full review for simple documentation errors on drawings should not be mandated.

2.6. The SNS-OPM-ATT 3.A-8.2a record to allow maintenance of the MEBT beam stop was reviewed. This form and its final signoffs should be a controlled document. Test procedures generated should be "codified" to allow use during future maintenance activities.

2.7. Identify routine "like for like" replacement and maintenance tasks. Generate procedures to perform such tasks on defined equipment (for example changing switches, indicators, etc.) with specified testing.

2.8. On forms SNS-OPM-ATT 3.A-8.1.a and SNS-OPM-ATT 3.A-8.2a include a "print name" with all signatures.

2.9. Define "commissioning," "certification" and "integration testing."

2.10. On SNS-OPM 3.A-7.4.12B "Initial steps of HEBT portion of PPS Phase 4.0 certification" step B.1.4 and SNS-OPM 3.A-7.4.12.A "Initial steps of Linac portion of PPS Phase 4.0 Certification" step A.1.4 calls for the PPS Engineer to verify the programs running in Chain A and Chain B match those stored on the Master CDs. Since "checksums" are not available from Controllogix, how is this done other than a program compare? Is there a special procedure written to cover the process used?

2.11. Validation and verification tests should be defined and consistently mandated and executed with specified and clear thresholds.

2.12. Post-maintenance, commissioning, integration, and certification tests should be categorized appropriately to help ensure clarity when a test is needed, and what kind of test it should be.
2.13. The appropriate test to be executed is determined, on a case-by-case basis, by the PST leader and the team; a procedure to clarify this should be generated.
2.14. Test categories should be identified in a stand-alone document.
2.15. Consider establishing a Test Director function for CECs.
2.16. Software media containing CEC PLC code should be physically stored in a safe.
2.17. Consider a CVS (Concurrent Version Management) system for CEC software code management.
2.18. There should be an acceptance test for replacement parts and new hardware for CEC components.
2.19. Cybersecurity implications (standalone plan, or integration with SNS IT cyber) should be considered for a network and for programmable components used in or connected to CECs.

3. Configuration Management Procedure 9.A series
   3.1. Clarification of process steps in these procedures should be undertaken; in particular:
      3.1.1. Procedures as written do not match USI screening in practice; use of the USI form is prescribed, but there is no evidence that it is used to conduct screenings conducted under the procedures.
      3.1.2. Procedures do not currently specify who is responsible for conducting the USI screening; this responsibility should be clearly stated.
      3.1.3. Section 5.10 of Procedure 9.1-3 appears to describe how the CCC conducts its review; its inclusion in the procedure appears to compromise CCC independence and may be in conflict with the CCC charter. Consider deleting this element of the procedure or re-wording to simply indicate that the CCC will conduct a review under its own processes.
      3.1.4. In the current form, the procedures specify the SE as the sole determiner of whether a CCC review is required for a proposed change. This decision should be made by line management, with consultation and concurrence by the SE.
      3.1.5. The decision matrix in Appendix C for determining what type of review is required for proposed changes does not provide a clear definition of the review types that apply (first column of table). The levels of review should be defined, so a consistent basis for these determinations is assured.
   3.2. For modifications to a CEC, independent technical advice should be sought, and this aspect should be ensured through the CCC process.

4. General Operating Procedures in OPM
   4.1. Periodic reviews and updates of procedures (e.g., SBMS specifies a 5-year review cycle, the SNS OPM specifies a 3-year review cycle) have not been performed for many procedures. These reviews should be completed as soon as feasible, as omission of these reviews is a deviation from SBMS requirements.
   4.2. The meaning of signatures on records needs clarification (technical review and approval). See, for example, Item 2, above.
   4.3. Several procedures necessary for assuring configuration management currently do not exist and should be implemented:

4.3.1. Delegation of Authority – This would provide processes for clear assignment of Research Accelerator Division director line management responsibility and authority for specific aspects of change control, including the event that the DD is not available for any reason.

4.3.2. Acceptance testing and storage of CEC parts – These procedures would define processes for ensuring that delivered CEC parts conform to specifications and function, as well as providing storage protocols that ensure parts are clearly identified by model, version, and other characteristics relevant to their function in the CECs.

4.3.3. Version control for software and firmware on PLCs used in CECs – This procedure would formally establish processes for storage, marking, access control, and other software quality/cyber security measures necessary to ensure that firmware and software used in CEC PLCs is identified and used in accordance with the correct version specifications.

4.4. It is not clear how the OPM procedures are intended to apply to ISD activities and personnel. This protocol should be codified, so that it is clear when ISD personnel are expected to operate under the OPM processes.

5. Configuration Control Committee

5.1. Consider supplementing composition of the committee by adding the Safety Documentation Manager and other technical specialists. This would ensure that potential safety basis impacts of proposed changes are identified and analyzed properly early in the change life cycle. Other technical specialists could help validate proposed testing following a change.

5.2. The role of the CCC in activities being conducted by ISD is not specified; this should be clarified in the applicable ISD and CCC process descriptions.

5.3. The meaning of signatures on records needs clarification (technical review and approval). See, for example, AR 2.

5.4. Clarification and codification of the CCC review life cycle is necessary to document the processes used to satisfy the committee charter, as well as to provide guidance for persons submitting proposed changes to the committee for review. Charting of process steps, analogous to the suggestion in Item 2, above, may be useful in this context.

5.5. Clarify if a single CCC applies to all SNS Divisions or if each Division is to establish a CCC.

5.6. The CCC should review systems against cyber security risks.

6. Training

6.1. The scope of training for several positions should be expanded to ensure personnel are fully effective in the roles and responsibilities assigned to them in the SNS configuration management/change control processes. In particular. provide:

6.1.1. Safety basis training for System Engineers, QA/QC, CCC members, Protection Systems Group

6.1.2. CCC process training for System Engineers and staff who implement modifications

6.2. Identification of training requirements for new or revised procedures (i.e., when training or re-training of personnel is required following change implementation) is not consistent and is not clearly codified. OPM processes for change control should provide guidance on when such training is necessary to address CEC or other significant modifications to equipment or processes.

6.3. Training profiles should be reviewed to assure all personnel working on systems (including craft) are aware of CEC labeling and requirements for accessing racks, enclosures, or cabling.

7. Independent Review
   7.1. Independent reviews are not fully implemented for CEC design changes, testing procedures and test results; provisions for these reviews and documentation of the results (e.g., tracking to resolution) should be incorporated into the OPM configuration management processes. These processes should include specifications for the independent review of post-change test plans and procedures for CEC modifications.
   7.2. The requirements for an independent review, performed by personnel outside the Protection Systems group, should be based on the nature and scope of the modification to the CEC. This can be determined between the System Engineer, Protection Systems Team Leader, USI screener, and CCC chair.

8. Contractor Assurance
   8.1. Contractor assurance processes are not clearly defined for OPM procedure modifications or for CEC modifications and post-change testing. To address this, consider adding QA sign-off to procedures and QA verification/vetting of key aspects of configuration management processes (e.g., verifying independent technical review, verifying tests were performed by technically qualified individuals, and verifying procedure modifications are being implemented and trained on as intended by management). QC resources could be deployed to support the technical component of QA responsibility. Qualified technical SNS staff could be assigned QC roles to perform the tests associated with modification that ensure conformance to established specifications. As noted in Item 6, above, additional training of QA/QC staff will be required to implement this approach to contractor assurance.
   8.2. Contractor assurance processes are not integrated into the CCC, OPM and CEC processes. That is, there are no procedure steps to identify deficiencies and opportunities for improvement, report deficiencies to the responsible manager, complete corrective actions and report lessons learned effectively across all aspects of SNS operation.

9. CEC Requirements Document
   9.1. A requirements document for in-house protection systems (PPS, ODH, instrument safety systems, personnel access systems) should be developed and formally issued for high-hazard accelerator enclosures. The document would specify high-level requirements for functionality and for processes (e.g., independent review) and documentation that would be maintained on these systems (e.g., code, wiring diagrams).

10. R2A2s
    10.1. Responsibilities and authorities of personnel with functional responsibilities in the SNS configuration management process need to be formalized and managed as controlled documents. In particular, those for the following positions should be addressed:
       10.1.1. CEC system engineer (see also Item 6)
       10.1.2. Quality assurance representative (see also Items 6 and 8)

ASSESSMENT CONCLUSIONS

Based on the Assessment Results presented herein, the Assessment Review Team concludes that SNS management understood the importance of CM and that CM was understood and accepted by SNS staff. There was clear evidence that CM procedures are being implemented. Corrective actions completed in response to the ORPS event were effective in improving the CM process. There was management commitment to improving CM processes, which was demonstrated by the existence of a "NScD Operational Quality and Efficiency Improvement Plan."

Also based on the Assessment Results, the Team developed 17 recommendations to improve effectiveness of CM for SNS CECs. For specific improvements, please see Recommendations listed in the Executive Summary.

APPENDIX A - ASSESSOR BIOGRAPHICAL INFORMATION

Edward T. Lessard has more than 35 years' experience with BNL providing safety management and technical services in the areas of radiation safety and accelerator safety. He was elected to BNL's scientific staff in 1988. Current positions include: Associate Chair of Environment, Safety, Security, Health and Quality, Collider-Accelerator Department (C-AD), and Chief Operating Officer for C-AD for the Nuclear and Particle Physics Directorate. He has participated in and/or led safety reviews for accelerators and research machines at other national laboratories (e.g., SNS, NSTX, ALS) and accelerators and accelerator facilities at BNL (e.g., NSLS II, ATF, BLIP, NSRL). Prior to that Mr. Lessard was principle investigator for BNL's Marshall Islands radiation safety project and for several NRC projects related to the development of internal dosimetry methods. For the past 25 years, Mr. Lessard has managed conduct-of-operations, occupational safety and health, and environmental management programs for the C-AD accelerator complex, which is the largest accelerator complex in the US. In addition, Mr. Lessard manages 30 FTE employed in the C-AD ESSHQ Division who provide training, radiation safety, work control, engineered safety system review and configuration management services. He has provided input to several DOE Orders (Conduct of Operations Order, Safety of Accelerator Facilities Order) and he chairs several Laboratory Committees (BNL ESH Committee, BNL Pressure and Cryogenics Safety Committee). He has an associate in nuclear engineering degree from Hartford State Technical College, a bachelor of radiological sciences and protection degree from Lowell Technological Institute and an M.S. degree in radiological sciences from the University of Lowell.

Enzo Carrone is Director of the Instrumentation and Controls Division at SLAC National Accelerator Laboratory, where he is responsible for machine sensors, networks, feedback systems, SCADA, HMI and safety systems (full product lifecycle, 90 staff). He was also Head of Radiation Safety Systems Department (Personnel Protection and Beam Containment), where he introduced the first distributed architecture on site (based on safety networks), the first integration of fast- and slow- controls for safety interlocks, as well as an integrated approach to project management and assurance (instituting Project Management Office and Change Control Board). In addition to experience in research environments, Dr. Carrone was also VP of production and business development manager in the Medical Technology industry. He received his M.SC. in Electrical Engineering from Polytechnic of Bari, Italy, and also his Ph.D. in Physics from the same Polytechnic and CERN (European Organization for Nuclear Research) in Geneva, Switzerland, where he designed control systems for particle physics detectors installed in the Large Hadron Collider (LHC). Enzo has experience in process control for large particle experimental facilities, as well as Project Management and leadership of international, multidisciplinary teams, operations of industrial plants, process optimization and turnaround management. He is an IEEE member and past-Executive Committee officer, a CERN past-Fellow, reviewer for DOE projects and associate editor of the International Journal on Modeling and Optimization.

John Forrestal has been with the Advanced Photon Source at Argonne National Laboratory for 24 years. He was responsible for the original design, implementation, and validations of the five Access Control and Interlock Systems (ACISs) at the APS. Currently he is responsible for the continuing operation and modification the ACISs, and is involved with the development of ACIS upgrades to support the next generation Storage Ring at the APS. He has participated in numerous design reviews of personnel

safety interlock systems of accelerator facilities at other national laboratories (such as Fermilab's Injector, Brookhaven's RHIC and NSLS-II, Thomas Jefferson Laboratory's 12 GeV upgrade of the CEBAF, Stanford Linear Accelerator Center's Linac Coherent Light Source, and Lawrence-Berkley Laboratory's Advanced Light Source) as well as serving on several accelerator review committees. Previously he was a project engineer at R.E. Timm and Associates responsible for the design and implementation of intrusion detection and delay systems to protect high value assets. Primary clients were the Department of Energy and the Department of Defense

Natasha Blair is a technical advisor for the Integrated Operations Support Division within Facilities and Operations at ORNL. She is also the ORNL Subject Matter Expert for Configuration Management. Previously, Natasha was technical advisor for the Engineering and Environmental Management group in the Nonreactor Nuclear Facilities Division (NNFD) at ORNL. She has approximately 19 years of experience in startups and readiness assessments in the DOE/National Nuclear Security Administration environment in accordance with DOE Order 425.1, including 8 years at ORNL and 11 years at Y-12 National Security Complex. In addition to readiness assessments for NNFD, she has participated in readiness assessments throughout the DOE Complex, including serving on the Management Self-Assessment for Cold Source Startup at the High Flux Isotope Reactor at ORNL and the Contractor Operational Readiness Review for the Highly Enriched Uranium Materials Facility at Y-12. Additionally, she has conducted several nonnuclear startup reviews, including reviews of mercury target change out for the Spallation Neutron Source at ORNL and the Operational Capabilities Assessment for the Biomass Steam Plant at ORNL. She maintains qualifications as an ORNL Lead Auditor.

John Young has been with the Department of Energy's Oak Ridge National Laboratory Site Office since 2010, and has participated in multiple assessments covering subject areas such as Electrical Safety, Lockout/Tagout, Hoisting and Rigging, Assessment Program, and Work Control. John has a Bachelor of Science degree in Electrical Engineering from Tennessee Technological University in Cookeville TN. John also has experience in the areas of Project Management, Performance Evaluation, Grant Management, High Performance Building, and Construction.

Dr. Kyle Turner is a principal in the firm McCallum-Turner, Inc. Dr. Turner has more than 30 years of experience providing technical, business, and management consulting services to commercial industry and government. He has participated in or led more than a dozen Integrated Safety Management (ISM) system assessments at Brookhaven National Laboratory, Idaho National Laboratory, Lawrence Berkeley National Laboratory, the National Renewal Energy Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and the Stanford Linear Accelerator Center National Laboratory. Dr. Turner has led evaluations, including nuclear safety processes, procedure compliance, conduct-of-operations, configuration management and event causal analysis at multiple DOE and commercial facilities. Dr. Turner has evaluated the effectiveness of work planning and control systems for both research and development activities and maintenance and operations functions and has evaluated existing assessment processes and systems as mechanisms to improve organizational performance. He has also provided input to the design and implementation of ISM, work planning and control, corrective action management, facility operations and management, and nuclear safety processes and programs at

several national laboratories. He has a bachelor of electrical engineering degree and M.S. and Ph.D. degrees in nuclear engineering from the Georgia Institute of Technology.

APPENDIX B - STAFF INTERVIEWED

Kevin Jones – Research Accelerator Division Director
Karen White – Control Systems Group Leader
Kelly Mahoney – Protection Systems Team Leader
Aaron Coleman –Systems Engineer
Bill Stone – Systems Engineer
David Freeman – Safety Documentation Specialist
George Dodson – Maintenance Management and IS Manager
Mike Baumgartner – Mechanical, Target and Vacuum Systems Group Leader
Glen Johns – Accelerator Operations Manager
Martha Carpenter – Quality Assurance Representative
Doug Paul – DOE Site-office – Facility Representative

APPENDIX C - DOCUMENTS REVIEWED

- Research Accelerator Division – Organizational Chart dated 9/12/2014
- SNS-OPM 3.A-8.1 – Configuration Management Procedure for the Following Certified Credited Engineering Controls: Personnel Protection System (PPS), Oxygen Deficiency Hazard (ODH) System, Transfer Bay Access Control (TBAC), Service Bay Differential Pressure Monitoring System (SBDPMS) and Target Protection System (TPS)
- 102030100-ES0007-R01 – Spallation Neutron Source Credited Engineered Controls List
- 102030100-ES0009-R03 – Spallation Neutron Source Credited Engineered Controls System Engineers List
- SNS-OPM 9.A-1 - SNS - Configuration Management Policy
- SNS-OPM 9.A-2 – SNS System, Structure, Component or Software Development Procedure
- SNS-OPM 9A-3 – SNS System, Structure, Component or Software Change Procedure
- SNS R2A2s for SNS System Engineer, Area Engineer, Area Physicist, Field Engineer, Operations Engineer
- 102030103-ES0018-R02 – Spallation Neutron Source Final Safety Assessment Document for Proton Facilities
- 102030102-ES0016-R03 - Spallation Neutron Source Final Safety Assessment Document for Neutron Facilities
- 102030103-ES0016-R05 - SNS Accelerator Safety Envelope (ASE): for Full Power Operations of the Front End, Linac, Ring, Transport Lines, Beam Dumps and Target
- SNS 109090100-SR0001-R00 - Spallation Neutron Source - Systems Requirements Document for Personnel Protection System
- SNS 109090100-IC0001-R00 - Spallation Neutron Source - PPS Interface Control Document
- SNS-109090100SR0002R00 – Safety Requirement Specification for the Accelerator Personnel Protection System
- SNS 102030103-ES0005-R01 – SNS – Personnel Protection System Safety Basis and Basis for Selection of Personnel Protection System Safety Integrity Levels
- Committee Charters – Electrical Safety, Radiation Safety, Accelerator Configuration Control
- DCN - 104010203-CN0005 – HVCM IGBT Gate Driver Power Supply Upgrade
- DCN – RAD-8300-073 – RCCS DTL-2 Flow Reversal Piping Modification
- DCN – 109090200-CN001 – TPPS Primary Shutter 1 and 11 Control Modification
- DCN – 105090200-CN0002 – Extraction Kicker PLC Controller Upgrade
- DCN – RAD-8600-209 – Modification of Accelerator and Target PPS per PCR SNS-RAD-ICS-CM-0041
- ACTS 0.28733 - ORPS Report SC-ORO--ORNL-X10CHRIDGE-2013-0005, Discovery of Non-Operable Safety System during Testing
- ACTS 16911 - SNS PPS Consulting. Assisting in the evaluation and implementation of corrective actions related to the July 2013 PPS common mode failure event.
- ACTS 16952 - Hazard and Operability Study: SNS Personnel Protection Systems
- ACTS 16183 - Assessment of PPS system during Winter outage
- ACTS 16905 - Operational Quality and Efficiency Improvement Plan

- ACTS 16891 - Accelerator Safety Review Committee (ASRC) SNS Triennial Assessment (102030102-ES0072)
- USI Evaluation for Replacement of Stand-by Pumps and Manifold Connection Hoses in the Target Service Bay FSS Water Mist System (Jul 2014)
- USI Evaluation for BL11 and BL1 Primary Shutter Control Logic (Jun 2014)
- USI Evaluation for BL 16B VISION Secondary Shutter Deceleration Switches (Feb 2014)
- USI Evaluation for BL 1A USANS (Feb 2014)
- USI Evaluation for PPS Power Supply Wiring Modifications and Implementation of Watchdog Diagnostics to Mitigate Common Mode Failures (Dec 2013)
- DOE Approval Safety Analysis for Interim Resolution of USI (Aug 2013)
- USI Evaluation for the PPS Redundant 24-Volt Power Supply Failure (Aug 2013)
- USI Evaluation for Lack of HEBT Chipmunk Enabled-Ring in Power Permit Logic Functionality Check In PPS Certification Procedure (Aug 2013)
- USI Evaluation of CHL Cryogenic Test Facility (Jul 2013)
- USI Evaluation of Core Vessel Insert Leak (Jul 2013)
- USI Evaluation for Limited 1 of 2 EVS Fan Operability (June 2013)
- USI Evaluation for BL 3 SNAP Roof Panel Interlock change (Feb 2013)
- USID Evaluation of VTA and Associated Changes to RFTF Access Control and ODH Systems (Jan 2013)
- USI Evaluation for Permanent Removal of BL 1B NOMAD Roof Grating (Dec 2012)