



LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

Causal Analysis: LLNL Software Quality Assurance Program Does Not Meet DOE O 414.1D Standards and Procedures Requirements

G. S. Holman, D. M. Whitney

January 31, 2013

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

Causal Analysis Report

Identification Information

Title of event or issue analyzed: LLNL Software Quality Assurance Program Does Not Meet DOE O 414.1D Standards and Procedures Requirements

Organization: Management Assurance System
Organization (MASO) Report date: January 30, 2013

Subcontractor (if applicable) Not applicable

Date of Event/Issue November 19, 2012 eCAR #: Not applicable

IWS/PWS #: Not applicable Security Inquiry Report #: Not applicable

ITS #: 35429 Occurrence Report #: Not applicable

Authorizing Manager: C. De Grange Noncompliance Report #: NTS -2013-0001

Location where event/condition occurred: Building: _____ Room: _____ Other: Institutional SQA Program

System or equipment involved: Institutional Software Quality Assurance Program (ISQAP)

Causal Analysis Team

Cause Analysis Lead: Garry Holman (MASO/PARS)

Cause Analysis Team (if applicable):

Darrel Whitney (MASO/QAO/ISQAP)

Issue Description

Event/Issue/Problem Statement

An assessment conducted by the NNSA Safety Analysis Department (NA-SH-60) for the NNSA Livermore Site Office (LSO),¹ the results of which were transmitted to LLNL in the November 2012 Periodic Issues Report,² identified the following issues within the LLNL Institutional Software Quality Assurance (SQA) Program concerning identification and flowdown of requirements, software grading levels, and implementation of the SQA program by Laboratory organizations:

Issue ISS-ESH-11.5.2012-478197 (Deficiency): "The LLNL was not able to demonstrate how an equivalency has been established with the use of the selected set of IEEE Standards used to implement the LLNL SQA Program as required by DOE O 414.1C, Attachment 2, paragraph 5, and DOE O 414.1D, Attachment 4, paragraph 2.a.; there is no documentation of the gaps between the selected set of IEEE Standards and the CRD requirements as

required by DOE O 414.1D, Attachment 1, 1.c.”

Issue ISS-ESH-11.5.2012-478199 (Deficiency): “LLNL’s graded approach for establishing grading levels for safety software is not equivalent to the methodologies defined under DOE O 414.1D, 6h and DOE O 414.1D, Attachment 4; or consistent with the “Conformance Criteria” required by the IEEE Standards.”

Issue ISS-ESH-11.5.2012-478200 (Deficiency): “NMTP did not implement the contractual requirements of DOE O 414.1D with the use of the selected set of IEEE Standards used to implement the LLNL SQA Program as required by DOE O 414.1C, Attachment 2, paragraph 5; and DOE O 414.1D, Attachment 4, paragraph 2.a.”

Issue ISS-ESH-11.5.2012-478201 (Weakness): “The LLNL Safety Software (830 Software) List, dated 01/12/2012, did not provide all of the information required by DOE O 414.1D Attachment 4, 2.(a).2.”

These four issues consolidate the 19 findings of the NNSA assessment report

LLNL determined these issues to be noncompliances with DOE Nuclear Safety Requirements. The programmatic nature of the noncompliances warranted reporting to the DOE Noncompliance Tracking System (NTS).

Describe the activity that was in progress at the time of the event or discovery of the issue:

Not applicable. Causal analysis is for results of an independent external assessment.

Chronology of actions/conditions leading to the event or issue (including step-by-step sequence of events):

No timeline created.

Immediate and/or mitigating actions taken in response to the incident/event:

No immediate and/or mitigating actions specific to the PIR issues were necessary because an Emergency Management Operating Directive (EMOD) was already in place for the Safety Software List deficiencies reported in Noncompliance Tracking System report NTS—LSO-LLNL-LLNL-2012-0009, “Incomplete Quality Assurance Records for Alternate Versions of DOE Toolbox Software.” The actions in the EMOD appropriately address needed mitigating actions.

Analysis and Results

The analysis utilized the System-Problem-Cause (SPC) methodology. As described in the attached SPC analysis chart, the analysis was organized into four parts, each corresponding to one of the issues described in the LSO Periodic Issues Report. Each of these parts, in turn, identified a cause (or causes) for each of the NNSA assessment findings associated with that particular PIR issue. The total population of finding-specific causes was then examined to identify root causes for the identified SQA issues.

Analysis:

Causes – Root or Apparent:

Root Cause 1: At the programmatic (i.e., ISQAP) level, lack of formality in the interactions between LLNL and LSO resulted in inadequate or missing records of evidence that the ISQAP was reviewed against all DOE O

414.1D requirements. This allowed for misinterpretations on the part of LLNL regarding DOE O 414.1D requirements.

Root Cause 2: At the implementation level, the ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP, particularly for those organizations lacking SQA expertise of their own and for lower-risk applications.

Other causal factors

LLNL and NNSA had differing opinions regarding interpretation of DOE O 414.1D graded approach methodology.

LLNL and NNSA had differing opinions regarding interpretation of IEEE standards.

The Nuclear Materials Technology Program lacks SQA expertise within its own organization.

The rigor of ISQAP requirements for specific SQA records is too informal for low-risk software.

Describe the significance of the event or condition (what could have happened?)

The LLNL institutional SQA program did not meet the contractual requirements of DOE O 414.1D for Software Quality Assurance (SQA).

LLNL use of the selected IEEE Standards may not provide an equivalent level of quality assurance requirements as the NQA-1 standard required by DOE O 414.1D.

Human performance improvement results (if not included in the analysis):

No HPI analysis conducted.

Judgments of Need/Recommended Corrective actions

Recommended corrective actions are described in the attached Corrective Action Plan³ and in the SPC analysis chart are associated with the applicable underlying cause(s) for each assessment finding.

Lessons Learned

No lessons learned were identified at this time.

References

¹ National Nuclear Security Administration, "Lawrence Livermore National Laboratory Building 332 Fire Detection and Alarm System and Hydrogen Gas Control System Safety Software Final Report," Associate Administrator for Safety and Health, Safety Analysis Department NA-SH-60 (September 28, 2012).

² National Nuclear Security Administration, Livermore Site Office, letter COR-IM-11/15/2012-480131 dated November 19, 2012, from P. Hill (NNSA-LSO Technical Deputy) to T. Gioconda (LLNL Deputy Director) on the subject "Transmittal of Periodic Issues Report"

³ Lawrence Livermore National Laboratory, "830 Software Quality Assurance Corrective Action Plan (for Deficiencies ISS-ESH-11.5.2012-478197, ISS-ESH-11.5.2012-478199, ISS-ESH-11.5.2012-478200, and Weakness ISS-ESH-11.5.2012-478201)," Management Assurance Office (January 15, 2013). Tracked as Assessment 35429 in the LLNL Issues Tracking System (ITS).

Symptom-Problem-Cause Analysis

Software Quality Assurance Issues NNSA-LSO Periodic Issues Report (November 2012)¹

January 30, 2013

Issue ISS-ESH-11.5.2012-478197 (Deficiency): "The LLNL was not able to demonstrate how an equivalency has been established with the use of the selected set of IEEE Standards used to implement the LLNL SQA Program as required by DOE O 414.1C, Attachment 2, paragraph 5, and DOE O 414.1D, Attachment 4, paragraph 2.a. (F-1); there is no documentation of the gaps between the selected set of IEEE Standards and the CRD requirements as required by DOE O 414.1D, Attachment 1, 1.c. (F-2)"

Observable Symptom	Associated Problem(s)	Underlying Cause(s)
Finding F-1: ² "The LLNL was not able to demonstrate how an equivalency has been established as required by DOE O414.1C, Attachment 2, paragraph 5; and DOE O 414.1D, Attachment 4, paragraph 2.a."	"The DOE O 414.1D, Attachment 4, paragraph 2.a requirement allows for the grandfathering of DOE O 414.1C DOE-approved QAPs if they meet the requirement[s] that are used to define and establish the equivalency." LLNL believed it could "grandfather" the DOE-approved QAP for DOE O 414.1C and did not perform the evaluation to demonstrate equivalency. "Given the issues in the correspondence trail ... and the other criterion not met under this section of the report, grandfathering was not an option."	Lack of formal equivalency evaluation (addressed by CAP Action 2.1.1) ³ Lack of formal interaction with NNSA-LSO (addressed by CAP Action 2.5.1) Lack of formal approval of ISQAP by NNSA-LSO (addressed by CAP Action 2.5.2)

Observable Symptom	Associated Problem(s)	Underlying Cause(s)
	<p>“For the most part, IEEE Standards require that a ‘Conformance Criteria’ be met in order to declare that the IEEE Standard’s requirements have been met. The LLNL ISQAP does not utilize a concept that is consistent in applying the ‘Conformance Criteria’.”</p>	<p>LLNL and NNSA had differing opinions regarding interpretation of IEEE standards (addressed by CAP Actions 2.5.1 and 2.5.2)</p> <p>Lack of formal interaction with NNSA-LSO (addressed by CAP Action 2.5.1)</p> <p>Lack of formal approval of ISQAP by NNSA-LSO (addressed by CAP Action 2.5.2)</p>
<p>Finding F-2: “There is no gap analysis which demonstrates the equivalency of ASME NQA-1-2008 with the NQA-1a-2009 addenda (or a later edition), Quality Assurance Requirements for Nuclear Facility Applications, Part I and Subpart 2.7 and the selected set of IEEE Standards used to implement the LLNL SQA Program as required by DOE O 414.1D, Attachment 1, 1.c.”</p>	<p>“To date LLNL has not submitted or documented a gap analysis as required by DOE O 414.1D, Attachment 1, 1.c. to demonstrate how the set of IEEE Standards are equivalent to the then ASME NQA-1-200 and the now, ASME NQA-1-2008 with the NQA-1a-2009 addenda (or a later edition), Quality Assurance Requirements for Nuclear Facility Applications, Part I and Subpart 2.7 for Software Quality Assurance.”</p>	<p>Lack of formal equivalency evaluation (addressed by CAP Action 2.1.1)</p> <p>Lack of formal interaction with NNSA-LSO (addressed by CAP Action 2.5.1)</p> <p>Lack of formal approval of ISQAP by NNSA-LSO (addressed by CAP Action 2.5.2)</p>

Possible corrective actions:

Corrective action mentioned in assessment report or directed by NNSA-LSO in PIR	LLNL Corrective action
<p>“It is recommended that NNSA LSO review and approve the grading levels and the graded approach as required by DOE O 414.1D, 5.c.(7) and Attachment 4, 2.a.(3).” (Assessment R-2)</p>	<p>LLNL to submit ISQAP to NNSA-LSO for approval (CAP Action 2.5.2)</p>

<p>“It is recommended that NNSA LSO implement the required exemption or equivalency process as described by DOE O 414.1D, 3.c. to revisit LLNL’s request for equivalencies regarding Software Quality Assurance.” (Assessment R-3)</p>	<p>LLNL to submit ISQAP to NNSA-LSO for approval (CAP Action 2.5.2)</p>
<p>“It is also recommended, that NNSA LSO evaluate the LLNL Implementation SQA Strategy to determine if LLNL is using a sound and cost effective approach in recognizing and using the IEEE Standards as the SQA Consensus Standard versus meeting ASME NQA-1-2008 with the NQA-1a-2009 addenda (or a later edition), Quality Assurance Requirements for Nuclear Facility Applications, Part I and Subpart 2.7.” (Assessment R-4)</p>	<p>LLNL to evaluate selection of a consensus standard (CAP Action 2.2.2). Action directed by NNSA-LSO.</p>
<p>LLNL shall perform a “Re-evaluation of LLNL's selection of consensus standards for the SQA program in the context of the standards' conformance criteria.” (Action directed by NNSA-LSO)</p>	<p>LLNL to re-evaluate selection of a consensus standard (CAP Action 2.2.2). Action directed by NNSA-LSO.</p>
<p>LLNL shall “Perform a revision to the Institutional Software Quality Assurance Program (ISQAP) based on the above [action], including developing documentation demonstrating that the LLNL SQA program provides an equivalent level of quality assurance requirements as NQA-1.” (Action directed by NNSA-LSO)</p>	<p>LLNL to document NQA-1 equivalency for 830 (i.e., safety) software (CAP Action 2.1.1). Action directed by NNSA-LSO.</p>
<p>“LLNL [shall] maintain all 10 CFR 830 software at its current risk level or higher until reevaluation under a revised ISQAP and risk grading methodology is approved by LSO.” (Action directed by NNSA-LSO)</p>	<p>LLNL will prevent use of the Process/Development Environment (PDE) risk report for lowering the risk level for future gradings of 830 software (CAP Action 2.2.1). Action directed by NNSA-LSO.</p>

Issue ISS-ESH-11.5.2012-478199 (Deficiency): “LLNL’s graded approach for establishing grading levels for safety software is not equivalent to the methodologies defined under DOE O 414.1D, 6h and DOE O 414.1D, Attachment 4; or consistent with the “Conformance Criteria” required by the IEEE Standards. (F-3, F-4)”

Observable Symptom	Associated Problem	Underlying Cause(s)
<p>“The LLNL ... graded approach methodology is orientated to consider risk and consequences that are associated ‘<i>project management risk associated with the successful completion of the software</i>’ which must be documented and controlled under DOE O 414.1D, SQA Work Activities - Risk Management.”</p>	<p>Finding F-3: "LLNL’s Institutional Software Quality Assurance Plan (ISQAP) safety software graded approach methodology is not equivalent to the graded approach methodology that is defined under DOE O 414.1D, 6h."</p>	<p>LLNL and NNSA had differing opinions regarding interpretation of DOE O 414.1D graded approach methodology (addressed by CAP Action 2.2.4).</p>
<p>The LLNL approach “is inconsistent with the graded approach as defined under DOE O 414.1D, 6.h. This graded approach is used by DOE and the NNSA to ensure that levels of analysis, documentation, and actions comply with requirements that are commensurate with:</p> <ul style="list-style-type: none"> “--the relative importance to safety, safeguards, and security; “--the magnitude of any hazard involved; “--the life-cycle stage of a facility or item; “--the programmatic mission of a facility; “--the particular characteristics of a facility or item; “--the relative importance to radiological and nonradiological hazards; and, “--any other relevant factors. (10 C.F.R. § 830.3)” 		

Observable Symptom	Associated Problem	Underlying Cause(s)
<p>“LLNL ISQAP Appendix A, Table 10., Risk Consequence Categories assumes a Design Basis Accident as Tier 0, (the highest level of consequence that safety software may experience), and Tiers 1 and 2 assume the loss of primary and secondary barriers, respectively.”</p>	<p>Finding F-4: "LLNL ISQAP safety software grading methodology is inconsistent with DOE O 414.1D, Attachment 4 and the 'Conformance Criteria' required by each of the IEEE Standards."</p>	<p>LLNL and NNSA had differing opinions regarding interpretation of DOE O 414.1D graded approach methodology (addressed by CAP Action 2.2.4).</p>
<p>“[The LLNL] ISQAP allows for the grading levels to be reduced by applying risk mitigation as a factor. Risk mitigation should not be used as a factor in the grading process.”</p>		<p>LLNL and NNSA had differing opinions regarding interpretation of DOE O 414.1D graded approach methodology (addressed by CAP Action 2.2.4).</p>
<p>“[The LLNL] ISQAP, Table 11. Process/ Development-Environment (PDE) Risks, is also used to as an additional tool to identify 'project development' risk that can also be used to reduce the grading levels.”</p>		<p>LLNL and NNSA had differing opinions regarding interpretation of DOE O 414.1D graded approach methodology (addressed by CAP Actions 2.2.1 and 2.2.4).</p>
<p>The LLNL ISQAP grading levels utilize “a level of documentation scheme which is not consistent with DOE O 414.1D or the set of IEEE Standards used as the consensus standard.”</p>		<p>LLNL and NNSA had differing opinions regarding interpretation of DOE O 414.1D graded approach methodology (addressed by CAP Action 2.2.4).</p> <p>LLNL and NNSA had differing opinions regarding interpretation of IEEE standards (addressed by CAP Actions 2.5.1 and 2.5.2)</p>

Possible corrective actions:

<p>Corrective action mentioned in assessment report or directed by NNSA-LSO in PIR</p>	<p>LLNL Corrective action</p>
<p>LLNL shall perform a “Re-evaluation of the grading level methodology and grading levels for all LLNL safety software in light of the report findings to ensure the appropriate safety SQA work activities are selected and implemented in accordance with the consensus standard.” (Action directed by NNSA-LSO)</p>	<p>LLNL shall evaluate and document integrated 830 software graded approach (CAP Action 2.2.4).</p>
<p>LLNL shall perform a “Revision to the Institutional Software Quality Assurance Program (ISQAP) based on the above [action].” (Action directed by NNSA-LSO)</p>	<p>LLNL shall update ISQAP documents (CAP Action 2.5.1). Action directed by NNSA-LSO.</p>
<p>“The revised ISQAP and safety software grading levels shall be submitted to LSO for approval.” (Action directed by NNSA-LSO)</p>	<p>LLNL shall submit updated ISQAP description document and associated procedures, forms and documents to LSO for approval (CAP Action 2.5.2). Action directed by NNSA-LSO.</p>

Issue ISS-ESH-11.5.2012-478200 (Deficiency): “NMTP did not implement the contractual requirements of DOE O 414.1D with the use of the selected set of IEEE Standards used to implement the LLNL SQA Program as required by DOE O 414.1C, Attachment 2, paragraph 5; and DOE O 414.1D, Attachment 4, paragraph 2.a.”

Observable Symptom	Associated Problem	Underlying Cause(s)
<p>Finding F-5: "Nuclear Materials Technology Program (NMTP) does not have implementing procedures to describe, document, and implement SQA lifecycle practices as required by ASME NQA-1-2008, Part I, Requirement 5."</p>	<p>Flowdown of requirements. ISQAP describes “what” organizations must do, organization procedures describe “how” the requirement is met. NMTP believed reference to ISQAP was sufficient to meet contractual requirements.</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p>
<p>“The FDAS MXL and HYDEC systems are categorized as safety significant SSCs in the Building 332 Documented Safety Analysis. The LLNL’s Safety Software (830 Software) List, dated 01/12/2012 recognized the FDAS MXL software and the HYDEC Safety PLC are listed as RL-3 and RL-4 safety software.</p> <p>“... the review would have expected to have seen the FDAS MXL software and the HYDEC Safety PLC graded as a DOE G 414.1-4 Level B, Configurable Software. That would have been equivalent to an RL-2 in the ISQAP; resulting having more SQA documentation in place for the two systems.”</p>	<p>Finding F-6: "NMTP did not properly categorize or grade the FDAS MXL software and the HYDEC Safety PLC as required by DOE O 414.1D."</p> <p>NMTP did not implement all aspects of ISQAP; or</p> <p>for those ISQAP aspects that were implemented, NMTP implementation was at an inappropriate level of rigor (i.e., at an inappropriate risk level); or</p> <p>the manner in which the NNSA assessor applied the IEEE standards (e.g., the “conformance clauses”) differed from that used by NMTP.</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p> <p>LLNL and NNSA had differing opinions regarding interpretation of DOE O 414.1D graded approach methodology (addressed by CAP Action 2.2.4).</p> <p>LLNL and NNSA had differing opinions regarding interpretation of the IEEE standards conformance clauses (addressed by CAP Actions 2.5.1 and 2.5.2).</p>

Observable Symptom	Associated Problem	Underlying Cause(s)
<p>Finding F-8: "NMTP did not meet the ISQAP requirement that requires that a Software Quality Assurance Plan be developed in accordance with IEEE 730-2002, IEEE Standard for Software Quality Assurance Plans for the FDAS MXL software."</p>	<p>NMTP did not implement all aspects of ISQAP; or</p> <p>for those ISQAP aspects that were implemented, NMTP implementation was at an inappropriate level of rigor (i.e., at an inappropriate risk level); or</p> <p>the manner in which the NNSA assessor applied the IEEE standards (e.g., the "conformance clauses") differed from that used by NMTP.</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p>
<p>"CMU09-000079, Rev AA, Software Quality Assurance Plan (SQAP) Hydrogen Gas System Weapons and Complex Integration, was reviewed based on IEEE 730-2002, IEEE Standard for Software Quality Assurance Plans. The document was found to be deficient and lacked specific and general information is required to demonstrate traceability of the product."</p>	<p>Finding F-9: "NMTP failed to develop and implement a SQAP in accordance with IEEE 730-2002, IEEE Standard for Software Quality Assurance Plans for the HYDEC Safety PLC."</p> <p>NMTP did not implement all aspects of ISQAP; or</p> <p>for those ISQAP aspects that were implemented, NMTP implementation was at an inappropriate level of rigor (i.e., at an inappropriate risk level); or</p> <p>the manner in which the NNSA assessor applied the IEEE standards (e.g., the "conformance clauses") differed from that used by NMTP.</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p>

Observable Symptom	Associated Problem	Underlying Cause(s)
<p>“IEEE 1228-94, Section 1.3, requires the creation of a written plan that addresses each topic, subtopic, and stipulation described in clause 4. The level of detail in, and the resources required by a software safety plan will be determined by factors including the type and level of risks associated with the software product, the complexity of the application, and external forces such as contractual requirements. The LLNL ISQAP SSP checklist format does not meet that requirement.”</p>	<p>Finding F-10: "NMTP failed to develop and implement a Software Safety Plan in accordance with IEEE Standard 1228-1994, IEEE Standard for Software Safety Plans, for the HYDEC Safety PLC and the FDAS MXL software."</p> <p>NMTP did not implement all aspects of ISQAP; or</p> <p>for those ISQAP aspects that were implemented, NMTP implementation was at an inappropriate level of rigor (i.e., at an inappropriate risk level); or</p> <p>the manner in which the NNSA assessor applied the IEEE standards (e.g., the “conformance clauses”) differed from that used by NMTP.</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p> <p>LLNL and NNSA had differing opinions regarding interpretation of IEEE standards (addressed by CAP Actions 2.5.1 and 2.5.2)</p>
<p>“NMTP indicated that their software configuration management was enveloped under the Facility’s Configuration Management System which is required by DOE O 420.1, Facility Safety and DOE–STD-073-2003. The Facility’s Configuration Management System was reviewed and failed to address IEEE Std 828-2005, Section 5, Conformance to the Standard, to consider it as equivalent to a safety software configuration management process.”</p>	<p>Finding F-11: "NMTP did not meet the requirement of IEEE Std 828-2005, ASME NQA-1-2009, Part I, Requirement 3, Section 802, and Part II, Subpart 2.7 Section 203, and DOE O 414.1D in establishing a Software Configuration Management Plans (SCMPs) for the FDAS MXL software and the HYDEC Safety PLC."</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p> <p>Lack of SQA expertise within NMTP (addressed by CAP Action 2.3.2).</p> <p>LLNL and NNSA had differing opinions regarding interpretation of IEEE standards (addressed by CAP Actions 2.5.1 and 2.5.2)</p>

Observable Symptom	Associated Problem	Underlying Cause(s)
<p>Finding F-12: "NMTP was unable to provide any formal documentation which describes the software requirements for the HYDEC Safety PLC and FDAS MXL as required by IEEE Std 830-1998, IEEE Recommended Practice for Software Requirements Specification, ASME NQA1-2008, Subpart 2.7, Section 400 and DOE O 414.1D."</p>	<p>NMTP did not have adequate records to demonstrate software traceability and software testing.</p>	<p>The rigor of ISQAP requirements for specific SQA records is too informal for low-risk software (addressed by CAP Action 2.2.3).</p>
<p>Finding F-13: "The System Design Documents for the FDAS and the Hydrogen Gas Control System do not describe general software and hardware information that is recommended by DOE-STD-3024-98, Content of System Design Descriptions, as per DOE O 420.1, Facility Safety."</p>	<p>NMTP disagreed with finding, alleged not a requirement. NMTP believed it was in compliance.</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p>
<p>Finding F-14: "NMTP does not have general Software Design Descriptions for the FDAS and the Hydrogen Gas Control System as required by IEEE Std 1016-1987, Recommended Practice for Software Design Descriptions, ASME NQA1-2008, Subpart 2.7, Section 400 and DOE O 414.1D."</p>	<p>LLNL and NNSA had differing professional opinions regarding interpretation of requirements.</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p> <p>LLNL and NNSA had differing opinions regarding interpretation of IEEE standards (addressed by CAP Actions 2.5.1 and 2.5.2)</p>

Observable Symptom	Associated Problem	Underlying Cause(s)
<p>Finding F-15: "NMTP was not able to demonstrate the traceability of software requirements and testing throughout the software lifecycle to ensure that the developed software for both applications as required by ASME NQA-1-2000/4/8/9, Part II, Subpart 2.7, Section 400."</p>	<p>NMTP did not have adequate records to demonstrate software traceability and software testing.</p>	<p>The rigor of ISQAP requirements for specific SQA records is too informal for low-risk software (addressed by CAP Action 2.2.3).</p>
<p>Finding F-16: "NMTP does not have a Software Verification and Validation Plan (SVVP) for the FDAS MXL software as required by ASME NQA-1-2000/4/8/9, Part II, Subpart 2.7, Section 400, DOE O 414.1D, and IEEE Std 1012, IEEE Standard for Software Verification and Validation."</p>	<p>Inadequate flowdown of requirements.</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p> <p>LLNL and NNSA had differing opinions regarding interpretation of IEEE standards (addressed by CAP Actions 2.5.1 and 2.5.2)</p>
<p>Finding F-17: "The recent FDAS MXL software modification and unit installation performed as per Change Request 332-12-027 was not performed in accordance with P/N 315-090380, MXL Control Panel Operations, Installation and Maintenance Manual, IEEE Std 1012, IEEE Standard for Software Verification and Validation, and ASME NQA-1-2008, Part II, Subpart 2.7, Section 400."</p>	<p>NMTP did not agree with the assessor's determination that the "software modification" constituted a "computer program change" as defined by NQA-1.</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p>

Observable Symptom	Associated Problem	Underlying Cause(s)
<p>ECMS No: CMU09-000074, Rev. AA, MCG Hydrogen Safety Shutdown Verification and Validation Plan, was submitted as the Software Verification and Validation Plan (SVVP) for the HYDEC Safety PLC. The document was found to be deficient in that it did not identify PLC software requirements or design specifications that would be tested during each of the life-cycle stages. There was no evidence in the SVVP that demonstrated that the PLC ladder logic was peer reviewed or tested prior to use. In general, the SVVP presented seemed to be the NMTP procedure that was used to system test the MCG Hydrogen System as a whole, rather than a document that would be used to demonstrate how software requirements and systems requirements are correct, complete, accurate, consistent and testable.</p>	<p>Finding F-18: "The CMU09-000074, Rev. AA, MCG Hydrogen Safety Shutdown Verification and Validation Plan does not meet the requirements of ASME NQA-1-2008, Part II, Subpart 2.7, Section 400, DOE O 414.1D, and IEEE Std 1012, IEEE Standard for Software Verification and Validation."</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p>
<p>There are no procedures in place that describe how software problem reporting and corrective actions are managed.</p>	<p>Finding F-19: "NMTP does not have a process in place to address software problem reporting and corrective action as defined and required by DOE O 414.1D and ASME NQA-1-2008, Subpart 2.7, Section 204."</p>	<p>ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL organizations when implementing the ISQAP (addressed by CAP Actions 2.2.3, 2.3.2, and 2.3.3).</p>

Possible corrective actions:

<p>Corrective action mentioned in assessment report or directed by NNSA-LSO in PIR</p>	<p>LLNL Corrective action</p>
<p>“The NNSA LSO [should] formally request procurement documents from LLNL to assess procurement specifications to ensure that Title 10 of the Code of Federal Regulations (CFR) Part 830, Subpart A, Criterion 7 items (1) and (2) have been met – given that the B332 DSA classifies the FDAS MXL software and the HYDEC Safety PLC as safety significant Structures Systems and Components (SSCs).” (Assessment R-5)</p>	<p>Recommendation made to NNSA-LSO. NNSA-LSO chose to not accept recommendation, therefore no LLNL corrective action.</p>
<p>“The LLNL contract [should] be reviewed [by LSO] to ensure that the requirements cited by DOE O 414.1D for Safety Software are in the LLNL Contract (i.e., ASME NQA-1-2008 with the NQA-1a-2009 addenda (or a later edition), Quality Assurance Requirements for Nuclear Facility Applications, Part I and Subpart 2.7, and the set of approved IEEE Standards).” (Assessment R-6)</p>	<p>Recommendation made to NNSA-LSO. No related LLNL corrective action at present.</p>
<p>LLNL shall “Perform a formal evaluation of all safety software used by NMTP to ensure there is no potential impact on operability of systems, structures, and components, e.g., unidentified failure modes, and there is no potential impact to the facility safety basis based on inadequate SQA,” (Action directed by NNSA-LSO)</p>	<p>NMTP will perform a formal analysis of potential impact (CAP Action 2.3.1). Action directed by NNSA-LSO.</p>
<p>LLNL shall “Perform an extent of condition [evaluation] reviewing implementation of SQA across the institution, e.g., Directorate implementing procedures and practices, and identification and resolution of any gaps identified in Directorate implementation of LLNL SQA requirements.” (Action directed by NNSA-LSO)</p>	<p>LLNL will perform an extent-of-condition evaluation (CAP Action 2.3.2). Action directed by NNSA-LSO.</p> <p>LLNL will develop additional corrective actions as appropriate (CAP Action 2.3.3). Action directed by NNSA-LSO.</p>

Issue ISS-ESH-11.5.2012-478201 (Weakness): “The LLNL Safety Software (830 Software) List, dated 01/12/2012, did not provide all of the information required by DOE O 414.1D Attachment 4, 2.(a).2. (F-7)”

Observable Symptom	Associated Problem	Underlying Cause(s)
<p>Finding F-7: “The LLNL Safety Software (830 Software) List, dated 01/12/2012, did not provide all of the information required by DOE O 414.1D Attachment 4, 2.(a).2.”</p>	<p>“Examples of information not listed include the description of the software (defined as software and firmware), the software names, and version identifiers.”</p>	<p>Same as identified in the root cause analysis for the Safety Software List noncompliance reported in NTS—LSO-LLNL-LLNL-2012-0009, “Incomplete Quality Assurance Records for Alternate Versions of DOE Toolbox Software.”⁴</p> <p>Root Cause: Changes between DOE O 414.1C and 414.1D were misunderstood, not adequately identified and addressed, and the requirement was not included in the SQA implementation plan.</p> <p>Root Cause: The ISQAP document to address requirements for compliance with DOE O 414.1D is written at a high level and focuses on the “what” as opposed to the “how” [for preparing and maintaining the LLNL Safety Software List].</p>

Possible corrective actions:

Corrective action mentioned in assessment report or directed by NNSA-LSO in PIR	LLNL Corrective action
The assessment report made no recommendations and NNSA-LSO did not direct any corrective actions regarding this specific issue.	LLNL currently addressing this issue through actions described in noncompliance report NTS—LSO-LLNL-LLNL-2012-0009.

REFERENCES:

¹ National Nuclear Security Administration, Livermore Site Office, letter COR-IM-11/15/2012-480131 dated November 19, 2012, from P. Hill (NNSA-LSO Technical Deputy) to T. Gioconda (LLNL Deputy Director) on the subject “Transmittal of Periodic Issues Report”

² Findings from National Nuclear Security Administration, “Lawrence Livermore National Laboratory Building 332 Fire Detection and Alarm System and Hydrogen Gas Control System Safety Software Final Report,” Associate Administrator for Safety and Health, Safety Analysis Department NA-SH-60 (September 28, 2012). Note in the assessment report that for Findings 6 and above listed in Table 1, there is an editorial error in correlation between the table entries and the respective finding descriptions in the text (i.e., finding F-6 in the table is listed as finding F-7 in the text). There is no finding labeled F-6 in the report text.

³ Corrective actions from Lawrence Livermore National Laboratory, “830 Software Quality Assurance Corrective Action Plan (for Deficiencies ISS-ESH-11.5.2012-478197, ISS-ESH-11.5.2012-478199, ISS-ESH-11.5.2012-478200, and Weakness ISS-ESH-11.5.2012-478201),” Management Assurance Office (January 15, 2013). Tracked as Assessment 35429 in the LLNL Issues Tracking System (ITS).

⁴ L. Soler, “Causal Analysis Report: Insufficient Safety Software Inventory List Documentation,” Lawrence Livermore National Laboratory, Quality Assurance Office, Report LLNL-AR-607472 (December 7, 2012)