DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Washington, DC 20004-2901

January 5, 2024

The Honorable Jill Hruby
Administrator
National Nuclear Security Administration
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Administrator Hruby:

The Defense Nuclear Facilities Safety Board (Board) recently completed a review of continuous air monitors (CAM) that are being upgraded at Lawrence Livermore National Laboratory's (LLNL) Plutonium Facility. The review focused on the software quality assurance (SQA) associated with the firmware for these monitors. These monitors are an essential part of the LLNL glovebox safety strategy to alert workers of airborne radioactivity.

The Board also reviewed a recent report by the Department of Energy's Office of Enterprise Assessments entitled *Independent Assessment of the Management of Safety Issues at the Lawrence Livermore National Laboratory*, which identified similar issues with SQA. LLNL and the Livermore Field Office have taken steps to address the quality assurance issues associated with CAMs in the Plutonium Facility.

The enclosure contains additional details on the review and provides the National Nuclear Security Administration and LLNL with additional information to use going forward to further improve SQA practices at the Plutonium Facility.

Sincerely,

Joyce L. Connery
Chair

Enclosure

c: Mr. Joe Olencz

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Report

October 26, 2023

Software Quality Assurance (SQA) of Continuous Air Monitors (CAM) for the Lawrence Livermore National Laboratory (LLNL) Recovery Glovebox Line

Summary. Members of the Defense Nuclear Facilities Safety Board's (Board) staff recently completed a review of the CAM upgrade activities at LLNL's Plutonium Facility. The CAM upgrade includes changes to software that controls all functions performed by the CAMs. These monitors are an essential part of the LLNL glovebox safety strategy to alert workers of airborne contamination. The staff review team concludes that SQA practices at the LLNL Plutonium Facility could be improved.

Background. LLNL employs CAMs in the Plutonium Facility to monitor for airborne radioactivity that may be inhaled by personnel, limiting potential exposure to alpha and beta contamination leakage from nearby gloveboxes. LLNL employs several such monitors in each room. The documented safety analysis (DSA) for the Plutonium Facility [1] credits the room CAMs as safety-significant components whose safety function is to detect airborne radioactive contamination and alert personnel. The DSA specifies the use of Canberra iCAMs^{TM} to perform this safety function.

The LLNL contractor, Lawrence Livermore National Security, LLC (LLNS), is in the process of replacing and upgrading nearly all the CAMs in the Plutonium Facility over the next several years. These upgrades will maintain the current local and remote CAM alarm notification functions while providing enhanced data gathering capability. The enhanced capabilities include CAM status monitoring with the capability to identify the individual CAM that is alarming without needing to physically enter the room in which the CAM is located; and the capability to acquire real time and archived data from the CAMs using new hardware and software. While these upgrades will not directly affect the credited safety functions, some modification to the CAM hardware and software is required to accommodate these upgrades.

Discussion. Firmware for the iCAMs did not appear on the safety software inventory list required by Department of Energy (DOE) Order 414.1D, *Quality Assurance* [2]. The iCAM firmware is software that is embedded into each iCAM to perform the "intelligent" functions required of the iCAM. This firmware constitutes safety software as defined by DOE Order 414.1D, paragraph 6.u. Management of such safety software includes, among other requirements, listing certain information on a safety software inventory, including software description, software name, version identifier, safety software designation, grade level designation, the specific nuclear facility application where the software is to be used, and the individual responsible for maintenance and application of the software.

LLNS refers to such software as "830 Software" and provides additional details on the definition of such software in RID-3103, *LLNL Interpretation of Safety Software (aka 830 Software)* [3]. The definition of 830 Software in RID-3103 is equivalent to the definition of safety software in DOE Order 414.1D. LLNS should have appropriately applied the requirements in RID-3103 to the iCAM software as discussed further below.

LLNS developed DES-0115, *LLNL Quality Assurance Program* (QAP) [4], to meet the contractor requirements for DOE Order 414.1D. DES-0115, Section 3.2.12, *Safety Software Quality Assurance Requirements for Nuclear Facilities*, establishes the responsibilities and processes for acquisition, design, development, modification, control, and/or use of safety software.

The National Nuclear Security Administration's Livermore Field Office approved the contractor's quality assurance plan, which establishes the framework for software engineering activities that include software specification, acquisition, design, development, verification and validation (including inspection and test), configuration management, maintenance, and retirement.

LLNS provides additional requirements for software quality assurance of 830 Software in DES-0111, *830 Institutional Software Quality Assurance Program* [5]; however, this document provides examples of exemptions by which software, including commercial firmware, can be exempted from LLNS's software quality assurance requirements. Specifically, the following applications, although meeting the definition of 830 Software, are exempted from the institutional software QAP:

1. *Equipment with embedded software that is covered under a Measuring & Test Equipment (M&TE) quality assurance program may substitute that program to satisfy the software quality assurance requirements of DOE Order 414.1D, Admin. Chg. 1; and*

2. *Commercially provided embedded software that cannot be tested separately from the equipment in which it is embedded, may be excluded from the Software Quality Assurance (SQA) program requirements provided the nuclear / radiological facility QA [quality assurance] program is applied to the equipment in which the software is embedded and that configuration control accounts for the firmware version number.* [5]

DOE's order on quality assurance requires, broadly, that American Society of Mechanical Engineers standard Nuclear Quality Assurance (NQA)-1 [6] be used in applications within DOE's nuclear facilities, which would include the iCAMs firmware. LLNS established the above exemptions based on implementation guidance provided in NQA-1. Subpart 2.7 of NQA-1 provides the quality assurance requirements for computer software for nuclear facility applications. Subpart 3.2-2.7 of NQA-1, Paragraph 101.6, provides the following optional, non-mandatory guidance for implementing the NQA-1 software quality assurance requirements (e.g., Subpart 2.7):

Firmware is dependent on the nature of the software and hardware device. Three possible approaches are described as follow:

a) *If the computer program can be changed after it is embedded, including at run time, all applicable controls of Subpart 2.7 should be applied.*

b) *If the computer program cannot be changed after it is embedded, and testing of the completed device is not adequate for full acceptance, Subpart 2.7 software development controls should be applied.*

c) *If the embedded computer program functions can be adequately verified by testing the completed unit and the computer program cannot be changed, including at run time, without repeating this verification, controls beyond those used for hardware may not be necessary. This approach is the least desirable because it treats software as hardware and does not recognize the need to apply controls to the computer program.*

Based upon this NQA-1 guidance, all applicable software quality assurance controls of Subpart 2.7 of NQA-1 should be applied to the iCAM firmware because it is designed such that operating parameters of the iCAM hardware can be changed after the firmware has been embedded into the hardware. However, LLNS uses the exemption provided by DES-0111 to exempt the iCAM firmware from 830 Software requirements. This M&TE exemption, LLNL-MI-834990 [7], declares that the iCAM firmware is covered under a QAP that may be substituted to satisfy the SQA requirements of DOE Order 414.1D. However, invoking the M&TE exemption for the iCAMs is inappropriate—while instrumentation used to calibrate the CAMs would be considered M&TE, the iCAMs themselves are not M&TE.

The iCAM firmware is of a nature that permits the user of the iCAM to configure operating characteristics that can affect the ability of the iCAM to accomplish its safety function. NQA-1 guidance therefore directs that applicable controls of Subpart 2.7 should be implemented.

LLNL Procedure 0124, *Control and Handling of Critical Measuring and Test Equipment* [8], establishes minimum requirements for handling M&TE. This document states that if "[t]he Critical M&TE is found to require any modifications or adjustments either to hardware or software…[then] See DES-0111, 830 Institutional Software Quality Assurance Program for additional information relating to software quality." Yet, DES-0111 specifically indicates that such M&TE equipment and software are exempted from those requirements. LLNS used this basis to determine that the iCAM firmware did not need to be placed on the safety software inventory as required by Order 414.1D. The net result is the iCAM firmware, which should be subject to the controls of NQA-1, Subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications*, is exempted from such controls by declaring the iCAMs to be M&TE.

A recent report by the DOE Office of Enterprise Assessments [9] came to several conclusions that substantiate elements of the staff review. Some key findings of the Enterprise Assessments report are:

- *Revision 11 of DES-0115…lacks quality assurance requirements equivalent to those in NQA-1.*

- *Since 2011, LLNS has not adequately invoked nearly all of the elements for quality assurance programs required by DOE to ensure nuclear safety and the timely identification and resolution of nuclear safety issues.*

- *Until the concerns identified in this report are addressed…significant uncertainties will exist regarding the impacts of quality assurance weaknesses on the safety of ongoing operations of LLNL nuclear facilities.*

Related Concerns. The staff review team identified several additional items during the execution of this review that further indicate the need for improvement in LLNS's SQA processes.

Miscalibration of Safety System Software—An Occurrence Reporting and Processing System report from last year [10] describes a technical safety requirement (TSR) violation resulting from miscalibration of the safety-significant criticality alarm system in the Plutonium Facility. While performing a semiannual surveillance requirement procedure on September 1, 2022, facility operators noted that an abnormal number of channels required recalibration. Upon review of the calibration documents and processes the following day, LLNS staff determined that a radioactive source used during the previous semiannual surveillance may not have been conservatively calibrated. This issue called into question whether the criticality alarm system would have alarmed at the TSR setpoint.

Federal Readiness Assessment (FRA) Findings on SQA—The National Nuclear Security Administration recently conducted an FRA to verify the readiness to restart some operations at the Plutonium Facility. The FRA report [11] identified several post-start findings related to SQA. The first finding was that contrary to the SQA plan, LLNS did not perform verification and validation tests after the software for a programable logic controller was changed. The second finding was that LLNS did not implement SQA procedures to meet the requirements of applicable consensus standards.

Conclusion. The staff review indicates SQA practices at LLNL need improvement. The requirements of NQA-1, Subpart 2.7, or equivalent, should be applied to the iCAM firmware. The iCAMs are not critical M&TE, and any exemption to DOE Order 414.1D requirements based on such characterization has no basis in the order. LLNL procedures related to SQA need to be corrected.

Since the staff team's review, LLNS has made some changes to the safety software inventory—the iCAM firmware is no longer listed on a separate Administrative Tab. The Livermore Field Office is reviewing the classification of the iCAM embedded software and other exemptions noted in SQA documents. LLNS is updating its SQA governing documents to address known deficiencies that have been identified over the past several years. This update is expected to be completed by May 2024.

References

[1] Lawrence Livermore National Laboratory Documented Safety Analysis, *Weapons and Complex Integration, Plutonium Facility-Building 332*, May 2017.

[2] Department of Energy Order 414.1D Chg 2 (LtdChg), *Quality Assurance,* April 25, 2011.

[3] Lawrence Livermore National Laboratory, *LLNL Interpretation of Safety Software (aka 830 Software),* RID-3103, Revision 3, July 17, 2017.

[4] Lawrence Livermore National Laboratory, *LLNL Quality Assurance Program*, DES-0115, Revision 11, April 2, 2021.

[5] Lawrence Livermore National Laboratory, *830 Institutional Software Quality Assurance Program*, DES-0111, Revision 02, September 15, 2017.

[6] American Society of Mechanical Engineers, *Requirements for Quality Assurance Programs for Nuclear Facilities*, NQA-1-2008, with the NQA-1a-2009 addenda.

[7] Lawrence Livermore National Laboratory, *ICAM Firmware_830 SQA Exemption*, LLNL-MI-834990, May 2, 2022.

[8] Lawrence Livermore National Laboratory, *Control and Handling of Critical Measureing and Test Equipment*, PRO-0124, Revision 05, October 8, 2021.

[9] Department of Energy Office of Enterprise Assessments, *Independent Assessment of the Management of Safety Isssues at the Lawrence Livermore National Laboratory,* April 2023.

[10] Occurrence Reporting and Processing System (ORPS), *B332 TSR Violation – Potential Discrepancies Impacting TSR Alarm Setpoints*, NA--LFO-LLNL-LLNL-2022-0037, September 2, 2022.

[11] National Nuclear Security Administration, *Final Report for the Federal Readiness Assessment Hydrogen Gas System/Metal Conversion Glovebox (UCNI)*, May 18, 2023.