DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Washington, DC 20004-2901

December 19, 2018

The Honorable James Richard Perry
Secretary of Energy
US Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0701

Dear Secretary Perry:

The Defense Nuclear Facilities Safety Board identified safety items with the safety basis for the U1a Complex at the Nevada National Security Site. These safety items include the heavy reliance on specific administrative controls, rather than engineering controls, to protect the experimental package and the lack of software quality assurance for the credited U1h Hoist Control System. These specific administrative controls do not effectively protect the experimental package from postulated insults. Failure of these controls during an accident could result in prompt death or serious injury of on-site personnel.

The Board acknowledges that the recent annual update for the safety basis includes a commitment to evaluate the feasibility of using an alternative container that may be credited as an engineering control for material movement activities. However, until it completes its evaluation, the U1a Complex will continue to rely on ineffective specific administrative controls during on-site material movements. The enclosed staff report summarizes the safety items and is provided for your information and use.

Yours truly,

Bruce Hamilton
Chairman

Enclosure

c: Mr. Joe Olencz

DEFENSE NUCLEAR FACILITES SAFETY BOARD

Staff Report

October 9, 2018

U1a Complex Safety Basis Review

Summary. Members of the Defense Nuclear Facilities Safety Board's (Board) technical staff reviewed the 2017 U1a Complex safety basis [1, 2]. This paper documents the potential safety items identified from that review. The Board's staff review team conducted the on-site portion of the review on June 12–13, 2018, at the Nevada National Security Site. The review team walked down the facility and held discussions with personnel from the National Nuclear Security Administration (NNSA) Nevada Field Office (NFO), Mission Support and Test Services, LLC (MSTS), Lawrence Livermore National Laboratory (LLNL), and Los Alamos National Laboratory (LANL). During its review, the staff review team identified the following potential safety items – safety observations:

1. *Lack of engineering controls for on-site material movements*: The 2018 annual update to the safety basis [3, 4] credits only specific administrative controls (SAC), rather than engineering controls, to protect the experimental package from thermal and electrical insults during on-site material movements;

2. *Lack of engineering controls for the experimental package when outside of the shipping container*: The safety basis does not identify engineering controls to protect the experimental package from mechanical insults when it is outside of the shipping container; and

3. *Lack of software quality assurance (SQA) for the U1h Hoist Control System*: SQA was lacking for firmware used to implement a safety significant control.

Background. The U1a Complex is an underground facility where NNSA fields and executes subcritical experiments (SCEs). SCE activities may comprise a series of both static (non-energetic) and dynamic (energetic, high-explosives driven) experiments using both radioactive and non-radioactive materials. Experiments in the U1a Complex use high explosives to generate high pressures that are applied to fissile materials for research and development purposes.

SCEs are assembled and packaged at the Device Assembly Facility (DAF) and transported to the U1a Complex. At DAF, the SCE is packaged into the device shipping container (DSC). The DSC, a metal box with ¼ inch thick walls and no insulation, was designed to transport the SCE from DAF to the U1a Complex. Upon arrival at the U1a Complex, workers offload the DSC from the truck, lower the DSC underground using the U1h shaft, and move the DSC to the Zero Room where the SCE is removed from the DSC. The Zero Room is the location in the U1a Complex where the SCEs are executed. Two plugs constructed of welded-steel beams and plates isolate the Zero Room from the rest of the U1a Complex during the execution of experiments. Both plugs are designed to withstand static overpressures that could result from the failure of the SCE vessel confinement system during experiment execution.

In September 2014, the previous management and operating (M&O) contractor, National Security Technologies, LLC (NSTec), found a non-conservative assumption in the safety basis regarding the release fraction used to estimate the consequences of postulated unmitigated accidents for a particular configuration of SCEs involving high explosives co-located with special nuclear material. Using a corrected airborne release fraction, NSTec analysts determined that the quantities of special nuclear material authorized for the U1a Complex exceeded the hazard category 2 threshold identified in Department of Energy (DOE) Standard 1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports* [5].

Per direction from NFO, NSTec, with the assistance of LANL and LLNL, revised the U1a Complex safety basis to reflect the hazard categorization upgrade from hazard category 3 to hazard category 2. NSTec prepared the revised safety basis in accordance with DOE Standard 3009-94, Change Notice 3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis* [6]. NFO reviewed the revised safety basis and approved it on March 15, 2017. The revised safety basis elevated the U1h Hoist Control System to safety significant and included two new limiting conditions for operation/surveillance requirements and 12 new SACs (7 were elevated from administrative controls). As part of the 2018 annual update [3, 4], the current M&O contractor, MSTS, re-analyzed the safety basis to account for the upcoming experiment. NFO approved the 2018 DSA annual update on September 12, 2018.

Members of the Board's staff reviewed the 2017 safety basis, which incorporated the hazard category change, and developed lines of inquiry on the process hazard analysis, accident analysis, credited control set, and technical safety requirements. In addition, the staff review team developed lines of inquiry on how the safety basis would change in the 2018 annual update.

Discussion. During its review, the staff team identified the following potential safety items – safety observations:

1. The 2018 annual update to the safety basis credits only SACs, rather than engineering controls, to protect the experimental package from thermal and electrical insults during on-site material movements;

2. The safety basis does not identify engineering controls to protect the experimental package from mechanical insults when it is outside of the shipping container; and

3. SQA was lacking for firmware used to implement a safety significant control.

1. *Potential Safety Item – Safety Observation: Lack of Engineering Controls for On-site Material Movements*—In the 2017 U1a Complex documented safety analysis (DSA) [1], the DSC was credited to protect the SCE package from mechanical, thermal, and electrical insults that could result in a high explosive violent reaction (HEVR) during transport. The DSA analyzed an HEVR, or a detonation of high explosives that are co-located to special nuclear material (i.e., the SCE), at the U1h collar to have the highest dose consequences. Mechanical, thermal, or electrical insults to high explosives may initiate an HEVR. For HEVR accidents at the U1a Complex, the DSA qualitatively determines that the unmitigated consequences to the

public and co-located worker would be low, but the consequences to the facility worker could include prompt death or serious injury.

In March 2018, MSTS declared a Potential Inadequacy of the Safety Analysis (PISA) related to the DSC in the U1a Complex DSA. In the current analysis, the DSA does not identify functional or performance criteria for electrical and thermal protection for the DSC. Furthermore, the staff team reviewed the design specification for the DSC and found no criteria related to thermal or electrical protection of the SCE package [7]. During the on-site portion of the review, MSTS informed the staff review team that the 2018 annual update would no longer credit the DSC with protecting the SCE package from thermal and electrical insults.

In the 2018 DSA annual update, MSTS credits four SACs, instead of the DSC, to protect the SCE package from thermal insults. The four SACs include the combustible material control, ignition source control, a control that limits concurrent activities, and a fire watch that encompasses all SCE operations. MSTS analysts concluded that crediting these four SACs adequately reduced the frequency for events associated with a fire involving the DSC transporting the SCE package.

The staff review team does not agree with the MSTS approach to credit only SACs to protect the SCE package from thermal insults. DOE Standard 3009-94, Change Notice 3, states, "The established hierarchy of hazard controls requires that engineering controls with an emphasis on safety-related SSCs [structures, systems, and components] be preferable to ACs [administrative controls] or SACs due to the inherent uncertainty of human performance." The DSC is an engineering control that could be credited to protect the SCE package from thermal insults, but MSTS does not have plans to verify that the DSC can provide thermal protection to the SCE package.

As for electrical protection, the 2018 DSA annual update analyzes two separate scenarios related to electrical insults to the SCE package: unintended application of electrical energy and lightning strikes. For both scenarios, MSTS no longer credits the DSC to protect the SCE package from electrical insults in the 2018 DSA annual update, but does require the use of high energy initiators for all SCEs. For scenarios involving the unintended application of electrical energy, MSTS credits the following four SACs: SCE operations walk down; limited concurrent activities; spotters; and critical lift. For the lightning strike scenario, MSTS reduced the initial frequency of the scenario based on lightning data recorded at the site and credits the severe weather restriction SAC (protects the experimental package from natural phenomena hazards, such as lightning) and the release-to-transfer SAC (test director ensures hazards are minimized during transfer of the experimental package to/from the U1a Complex).

The staff review team does not agree with the MSTS approach of crediting only SACs to protect the SCE package from electrical insults instead of following the preferred hierarchy of controls described in DOE Standard 3009-94, Change Notice 3. The DSC in conjunction with lightning-induced electromagnetic pulse (LIEMP) covers or shorting plugs for SCE detonators are engineering controls that could be credited to protect the SCE package from electrical insults. However, MSTS has not made plans to verify that the DSC can provide electrical protection to the SCE package, nor has MSTS required the use of LIEMP covers or shorting plugs.

During the on-site interaction with the staff review team, MSTS discussed the possibility of adopting a more robust container. The 2018 DSA annual update includes a commitment to evaluate the feasibility of using an alternative shipping container. NFO expects that MSTS will complete the evaluation by the end of fiscal year 2019. The staff review team concludes that adopting a more robust container and crediting it as an engineering control for multiple hazards would be an improvement in the control strategy and more consistent with DOE Standard 3009-94, Change Notice 3. However, until it completes its evaluation, MSTS will continue to rely on SACs to protect the experimental package from thermal and electrical insults during on-site transportation activities.

2. *Potential Safety Item – Safety Observation: Lack of Engineering Controls for SCE outside the DSC*—The 2018 DSA annual update analyzes a mechanical impact-induced explosion during underground operations when the SCE is outside of the DSC. The DSA analysis states that the frequency of an impact-induced explosion is judged to be extremely unlikely, in contrast to the frequency of unlikely that it used in general for other explosion scenarios. MSTS personnel informed the staff review team that this was due to the limited amount of mechanical equipment and overhead structures. The DSA describes the overhead equipment in the Zero Room, which includes light fixtures, crane/hoist support structures, ventilation/piping, and ground support equipment (i.e., rockbolts and shotcrete).

The staff review team concluded that the analysis is taking credit for the room structure during the unmitigated phase of the hazard analysis. In the DSA, the Zero Room Structure is only credited as a mitigative control (confinement of material). However, when describing the system, the DSA states, "Collectively, the use of rockbolts and application of wire-mesh fabric and Shotcrete on the ribs provide a 'finished' interior within the Zero Room (except for the 'Get Lost Region'). The attributes of this 'finished' interior reduce the likelihood that sidewall or overhead ceiling material could become loose or dislodged and subsequently cause a mechanical insult to exposed equipment or experiment-related items (e.g., an SCE)." The staff review team concludes that it is inappropriate to reduce the assumed frequency of the accident without crediting the room structure, which would include properly secured overhead equipment.

MSTS personnel informed the staff review team that further credited preventive measures were not required based on the accident progression and control selection. The current control set for this hazard consists of SACs for limited concurrent activities and qualified explosives handlers. Crediting the Zero Room structure for this hazard scenario would provide an engineering control. MSTS also could credit the Zero Room structure for mechanical insult hazard scenarios for other phases of SCE operations (e.g., DSC transportation, post-experiment vessel movement, and entombment).

3. *Potential Safety Item – Safety Observation: Lack of SQA for U1h Hoist Control System*—The 2018 DSA annual update credits the U1h Hoist Control System to prevent an explosion resulting from a runaway hoist malfunction at the top of the U1h shaft. If the U1h Hoist Control System failed to perform this function during SCE operations, the DSA qualitatively determines that the unmitigated consequences to the facility worker could include prompt death or serious injury. As part of the safety significant boundary of the U1h Hoist Control System, MSTS identifies the U1h Control System Programmable Logic Controller (PLC) Firmware [8]. The Hoist Control System uses two PLCs embedded with software (i.e., firmware), the Hoist Controller PLC and Ultimate Hoist Monitor PLC [9]. The Hoist Controller

PLC is programmed to apply the hoist mechanical brakes immediately if a system error in position or speed exceeds a predetermined value. The Ultimate Hoist Monitor PLC is programmed to monitor a subset of the Hoist Controller functions, including cage over-speed and cage over-travel sensing, by using data retrieved from redundant field sensors. The software that runs the program in the PLCs is necessary to ensure that the U1h Hoist Control System can perform its safety function.

MSTS personnel stated that the PLC firmware for the U1h Hoist Control System is treated as hardware and the SQA requirements listed in DOE Order 414.1D, *Quality Assurance* [10], do not apply. MSTS personnel further stated that the software embedded into the PLC is exempt from DOE Order 414.1D given that MSTS personnel will not change and cannot control the firmware. In addition, MSTS stated that the PLC firmware is tested and validated as part of the PLC (i.e., hardware), using the approved quality assurance and engineering procedures. The staff review team verified that this approach is permitted—but discouraged—by the American Society of Mechanical Engineers NQA-1-2008, *Quality Assurance Requirements for Nuclear Facility Applications* [11], which states, "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."

The staff review team does not agree with the MSTS approach of classifying the PLC firmware as hardware. DOE Guide 414.1-4, *Safety Software Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance* [12], defines the different types of software. The guide states, "Firmware is acquired software." The guide defines acquired software as "generally supplied through basic procurements, two-party agreements, or other contractual arrangements. Acquired software includes commercial off-the-shelf (COTS) software, such as operating systems, database management systems, compilers, software development tools, and commercial calculational software and spreadsheet tools."

DOE Order 414.1D defines safety system software as "software for a nuclear facility that performs a safety function as part of an SSC and is cited in either (a) a DOE-approved documented safety analysis; or, (b) an approved hazard analysis." As stated above, the safety significant U1h Hoist Control System PLCs are embedded with software that ensure the control performs its safety function. The staff review team concludes that the software embedded into the PLCs is acquired software and meets the definition of safety system software. Therefore, MSTS would be required to follow the graded approach in DOE Guide 414.1-4 for performing SQA work activities to be in compliance with DOE Order 414.1D.

The staff review team also does not agree with the approach of treating firmware as hardware given that NQA-1-2008 states that it is the least desirable. The U1h Hoist Control System is the only control credited to prevent an explosion resulting from a runaway hoist malfunction at the top of the U1h shaft. In addition, the U1h Hoist Control System was recently elevated to safety significant in the U1a Complex safety basis that addressed the hazard categorization change. Therefore, the previous and current M&O contractor had never performed the SQA activities required by DOE Order 414.1D for the software embedded in the PLCs. Even though MSTS tests and validates the PLC firmware by testing the function of the Hoist Control System, these activities will not identify potential flaws in the software.

Conclusions. During the review, the Board's staff review team identified the following potential safety items – safety observations:

1. *Lack of engineering controls for on-site material movements*: The 2018 annual update to the safety basis credits only SACs, rather than engineering controls, to protect the experimental package from thermal and electrical insults during on-site material movements;

2. *Lack of engineering controls for the experimental package when outside of the shipping container*: The safety basis does not identify engineering controls to protect the experimental package from mechanical insults when it is outside of the DSC; and

3. *Lack of SQA for the U1h Hoist Control System*: SQA was lacking for firmware used to implement a safety significant control.

The 2018 DSA annual update includes a commitment to evaluate the feasibility of using an alternative shipping container, which NFO expects to be complete by the end of fiscal year 2019. The staff review team believes adopting a more robust container and crediting it as an engineering control for multiple hazards would be an improvement in the control strategy and more consistent with DOE Standard 3009-94, Change Notice 3. However, until it completes its evaluation, MSTS will continue to rely on SACs to protect the experimental package from thermal and electrical insults during on-site material movements.

References

[1] National Security Technologies, LLC, *U1a Complex Subcritical Experiments Documented Safety Analysis*, U1a-SCE-DSA-001, Revision 1, Change Notice 1, February 2017.

[2] National Security Technologies, LLC, *U1a Complex Subcritical Experiments Technical Safety Requirements*, U1a-SCE-TSR-001, Revision 1, Change Notice 1, February 2017.

[3] Mission Support and Test Services, LLC, *U1a Complex Subcritical Experiments Documented Safety Analysis*, U1a-SCE-DSA-001, Revision 2, August 2018.

[4] Mission Support and Test Services, LLC, *U1a Complex Subcritical Experiments Technical Safety Requirements*, U1a-SCE-TSR-001, Revision 2, August 2018.

[5] Department of Energy, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, DOE Standard 1027-92, Change Notice 1, September 1997.

[6] Department of Energy, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis*, DOE Standard 3009-94, Change Notice 3, May 2006.

[7] Los Alamos National Laboratory, *Device Shipping Container Technical Specifications*, ESA-EDE-SP-05-0001, Revision C, February 2006.

[8] National Security Technologies, LLC, *Functional Classification Document: U1h Hoist Control System*, U1a-FCD-2016-001, Revision 3, January 2018.

[9] National Security Technologies, LLC, *System Design Description for the U1h Hoist Control System*, SDD-U1a.014, Revision 1, May 2018.

[10] Department of Energy, *Quality Assurance*, DOE Order 414.1D, Admin Change 1, May 2013.

[11] American Society of Mechanical Engineers, *Quality Assurance Requirements for Nuclear Facility Applications*, NQA-1-2008, March 2008.

[12] Department of Energy, *Safety Software Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*, DOE Guide 414.1-4, June 2005.