DEFENSE NUCLEAR FACILITIES SAFETY BOARD
Washington, DC 20004-2901

May 13, 2020

The Honorable Dan Brouillette
Secretary of Energy
US Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0701

Dear Secretary Brouillette:

The Defense Nuclear Facilities Safety Board has reviewed the hoist control system used for lowering subcritical experiments at the Nevada National Security Site's U1a Complex. This review identified several matters regarding the design and qualification of the system. The Board also communicated a matter regarding the system in its letter dated December 19, 2018. The Board recognizes that these issues exist because the system was not designed for a nuclear safety function and was only recently elevated in safety classification.

The Board notes that the NNSS contractor has issued a plan to evaluate the hoist systems at the U1a Complex. The evaluation will include identifying components that require replacement to enhance the systems' reliability or operability. The enclosed report describes safety matters regarding the current system and is provided to aid in the identification and execution of needed safety improvements.

Yours truly,

Bruce Hamilton
Chairman

Enclosure

c: Mr. Joe Olencz

DEFENSE NUCLEAR FACILITIES SAFETY BOARD
Staff Report

April 3, 2020

U1h Hoist Control System at the Nevada National Security Site's U1a Complex

Summary. Members of the Defense Nuclear Facilities Safety Board's (Board) staff reviewed the U1h hoist control system at the Nevada National Security Site's (NNSS) U1a Complex. The objective of the review was to ensure that the hoist control system could reliably perform its nuclear safety function, and that the system and its operation were in compliance with Department of Energy (DOE) directives. The Board's staff review team conducted a teleconference review on April 9, 2019, with personnel from the National Nuclear Security Administration's (NNSA) Nevada Field Office (NFO) and Mission Support and Test Services, LLC (MSTS), and reviewed additional information based on that discussion. During its review, the staff review team identified the following safety observations:

1. *Inappropriate Analysis of the Runaway Hoist Hazard Scenario*: The approved and implemented U1a Complex documented safety analysis (DSA) [1] uses failure rate data of the hoist control system when determining the uncontrolled frequency for the runaway hoist hazard scenario; and

2. *Potentially Inadequate Control Strategy for Runaway Hoist Hazard Scenario*: The approved and implemented U1a Complex DSA only credits the hoist control system to reduce the risk associated with the runaway hoist hazard scenario.

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 apply high pressures to fissile materials for research and development purposes.

In 2018, the Board's staff reviewed the U1a Complex safety basis. The DSA revision that the staff reviewed was the first to credit the U1h hoist control system for a nuclear safety function [2]. The safety significant hoist control system is the only implemented control credited to prevent an explosion resulting from a runaway hoist malfunction at the top of the U1h shaft. This scenario assumes that the hoist cage is carrying an experimental package that consists of special nuclear material and high explosives.

On December 19, 2018, the Board sent a letter [3] to DOE that communicated the Board's safety observations with respect to the U1a Complex safety basis. One of the safety observations discussed in the Board's letter was associated with the lack of software quality assurance (SQA) for the credited U1h hoist control system firmware. In 2019, the Board's staff performed a focused review on the hoist control system to evaluate if it could reliably perform its safety function, and if the system and its operation were in compliance with DOE directives.

In July 2019, while the staff team's review was in progress, MSTS declared a potential inadequacy of the safety analysis (PISA) on the ability of the hoist control system to stop the hoist cage from impacting the top or bottom of the shaft when traveling at full speed. As a result of this PISA, MSTS finalized a report in January 2020 [4] that analyzed the hoist control system and recommended changes to the U1a Complex safety basis. NFO had not approved the DSA change notice as of March 2020.

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

- The approved and implemented U1a Complex DSA [1] uses failure rate data of the hoist control system when determining the uncontrolled frequency for the runaway hoist hazard scenario; and

- The approved and implemented U1a Complex DSA only credits the hoist control system to reduce the risk associated with the runaway hoist hazard scenario.

Inappropriate Analysis of the Runaway Hoist Hazard Scenario—In the implemented and approved DSA [1], MSTS determined the uncontrolled frequency for the runaway hoist hazard scenario to be "Extremely Unlikely." MSTS made this determination by using an estimate of the number of yearly hoist operations with experiment packages, an approximate time needed for the hoist to lower the experiment package, and failure rate data for individual components of the hoist control system. By using the failure rate data in this determination, MSTS is taking credit for the hoist control system in the unmitigated analysis. DOE Standard 3009-94, Change Notice 3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses* [5], requires unmitigated analyses be evaluated without safety controls. By using a less conservative uncontrolled frequency, MSTS is underestimating the risk and undervaluing the risk reduction needed for the runaway hoist scenario.

In addition to crediting the hoist control system in the unmitigated analysis, the DSA credits the system as a preventive control to reduce the frequency to "Beyond Extremely Unlikely" for the mitigated analysis. The staff team concludes that it is inappropriate to take credit for the system twice. NFO and MSTS agreed with the staff team and stated that they were already preparing a change notice to the U1a Complex DSA that would no longer take credit for the hoist control system in the unmitigated analysis, thus resulting in an "Unlikely" uncontrolled frequency. The DSA change notice was in response to the PISA discussed above. NFO had not approved the DSA change notice as of March 2020.

Potentially Inadequate Control Strategy for Runaway Hoist Hazard Scenario—As discussed above, although the former NNSS contractor National Security Technologies, LLC, elevated the U1h hoist control system classification to safety significant in 2017, it was not designed, procured, or installed as a credited nuclear safety control.

In the approved and implemented U1a Complex DSA [1], the hoist control system is the only control credited to reduce the risk from the runaway hoist hazard scenario. In the hazard analysis, it provides a one-bin reduction in frequency (i.e., one to two orders of magnitude)

between the uncontrolled and controlled analyses. As a result, the DSA qualitatively determines the risk is low enough that additional safety controls need not be considered for this hazard.

Safety instrumented systems (SIS), such as the hoist control system, are instrumented systems that perform safety functions and should be designed and maintained in accordance with functional safety standards. Functional safety standards, such as American National Standards Institute (ANSI)/International Society of Automation (ISA) 84.00.01, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* [6], which is the national consensus standard referenced by DOE Standard 1195-2011, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities* [7], recommend that the SIS be independent of the basic process control system (BPCS), or the "lack of independence must be assessed and shown to be sufficiently low compared to risk reduction requirements. The following factors shall be included in this assessment: common cause failure of the SIS and the cause of demand; common cause of failure with other protection layers providing risk reduction; [and] any dependencies that may be introduced by common operations, maintenance, inspection, or test activities or by common proof test procedures and proof test times."

The U1h hoist control system performs both normal control and safety functions. Therefore, the SIS are not independent from the BPCS. MSTS has not performed an assessment to show whether the lack of independence is sufficiently low compared to risk reduction requirements. For a BPCS that also performs a safety function, ANSI/ISA 84.00.01 permits crediting a maximum of one order of magnitude risk reduction. However, since MSTS's proposed change notice to the U1a Complex DSA would update the uncontrolled frequency to "Unlikely", the credited controls would need to reduce risk for the runaway hoist scenario by three to four orders of magnitude. Therefore, unless MSTS can complete an assessment demonstrating that the lack of independence is sufficiently low compared to risk reduction requirements, the current implemented control strategy would not provide sufficient risk reduction for the runaway hoist hazard scenario. If greater risk reduction is required, the BPCS must be designed and managed to the requirements of functional safety standards, or additional protection layers must be identified.

In response to the July 2019 PISA, MSTS developed a report [4] that analyzed whether the U1h hoist control system could adequately prevent the unintended travel of the hoist cage beyond the shaft upper and lower stop locations. The report includes a safety integrity level (SIL) calculation. Application of Appendix B in DOE Standard 1195-2011 to the safety function of the BPCS results in a SIL requirement of SIL-2, which corresponds to a risk reduction in the range of 100 to 1000. As discussed above, the functional safety standards state that the BPCS cannot be credited for a risk reduction of this magnitude. Nevertheless, MSTS performed the SIL calculation in a manner that assumed that the software and hardware components of the SIS were completely independent of the BPCS. Using otherwise conservative assumptions, MSTS calculated the probability of failure on demand (PFD) to be 6.57E-03. This is a risk reduction of 148 which falls into the lower portion of the required SIL-2 range.

In this calculation, MSTS used an electrical diagram as the basis for a reliability block diagram. Such a diagram shows the relationship of various components in a reliability sense. The MSTS SIL calculation conservatively assumed that component failure rates were comprised

of 100 percent dangerous, undetectable failures. MSTS also appropriately accounted for an allowed 25 percent extension of surveillance or proof test intervals.

While MSTS did make an adjustment for potential common cause failures of some elements, the staff team found that MSTS did not include any adjustments for potential common cause failure of the two pulse encoders (used to derive cage position and hoist speed values) and did not consider any potential for common cause failures of the solid state output relays. The staff team also found that the reliability block diagram failed to include bypass relays, which have failure modes that would defeat the ability of the limit switch to signal a hoist overtravel position. Lastly, the report lists seven logic controls preventing overtravel and claims "the combination of controls ensure all overtravel requirements are met." However, only one of these controls directly provides protection independent of the programmable logic controllers (PLCs). The remaining six controls rely on the proper functioning of software and computer hardware, as well as two pulse encoders to determine cage position or hoist speed. These same elements are also potential initiators of the initiating hazard that requires mitigation.

MSTS is introducing a new specific administrative control (SAC) in the U1a Complex DSA change notice as a result of the PISA response report. The SAC will limit the hoist travel speed and is intended to ensure the hoist cage does not travel beyond the top and bottom of the shaft when carrying an experiment package. MSTS determined the SAC speed limit based on brake performance data collected at the time the hoist control system was installed but did not account for potential brake degradation over the life of the brakes or degraded brake performance that would occur if one of the redundant brake assemblies failed.

While MSTS has taken some actions, the staff team remains concerned with the control strategy for the runaway hoist hazard scenario. The staff team identified several concerns within the SIL calculation for the hoist control system that challenge the risk reduction MSTS can credit. Also, the new SAC would provide an additional layer of protection, but it is not independent as it still relies on the hoist control system to properly perform its function. Therefore, the staff team is concerned the risk for this hazard scenario has not been fully evaluated or sufficiently reduced.

U1a Complex Hoist Systems Evaluation Project—Due to the age of the hoist systems at the U1a Complex, MSTS has identified obsolescence issues and difficulties obtaining spare parts (e.g., PLCs for the U1h hoist control system). In March 2020, MSTS developed a statement of work [8] to hire a subcontractor to evaluate the hoist systems at the U1a Complex. Tasks for the subcontractor include identifying components that require replacement to enhance operability or reliability and providing technical recommendations for improvements to components/systems. MSTS will rely on the subcontractor's feedback to determine whether to replace components and subsystems of the hoist control system.

The U1h hoist control system was not designed for a nuclear safety function. With plans to evaluate the hoist systems at the U1a Complex and enhance their reliability, MSTS has the opportunity to address the staff team's concerns with the current U1h hoist control system by procuring a system that is compliant with DOE directives and industry standards. For example:

- As discussed in the report provided by the Board's letter of December 19, 2018, the staff review team concluded that the software embedded into the PLCs is acquired software and meets the definition of safety system software. The staff team also concluded that the software should not be exempt from the requirements in DOE Order 414.1D, *Quality Assurance* [9]. The statement of work for hoist systems [8] includes a task for the subcontractor to conduct technical evaluations for the firmware/software. The staff team believes this would be an ideal time for MSTS to follow the graded approach in 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* [10], for performing SQA work activities for the software on the PLCs to bring the system into compliance with DOE Order 414.1D.

- Likewise, this provides an opportunity for MSTS to separate the hoist control system from all components and systems that provide credited safety functions. The PLC that provides hoist control should not be relied on to perform credited safety functions. Safety functions requiring a PLC should be segregated in separate PLCs in accordance with requirements of the appropriate functional safety standards.

- A paper by Barkand [11] includes a discussion of emergency braking systems designed to provide ascending conveyance overspeed protection, which could be included in a new hoist control system. These include passive dynamic braking systems that use the regenerative braking capacity of the drive motor to provide a retarding force if the hoist braking system is lost in conjunction with a power loss to the hoist drive motor, independent hoist rope brake systems, and buffers to minimize contact forces.

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

1. ***Inappropriate Analysis of the Runaway Hoist Hazard Scenario***: The U1a Complex DSA uses failure rate data of the hoist control system when determining the uncontrolled frequency for the runaway hoist hazard scenario; and

2. ***Potentially Inadequate Control Strategy for Runaway Hoist Hazard Scenario***: The U1a Complex DSA only credits the hoist control system to reduce the risk associated with the runaway hoist hazard scenario.

Due to the age of the hoist systems at the U1a Complex, MSTS has identified obsolescence issues and difficulties obtaining spare parts. MSTS has developed a statement of work [8] to hire a subcontractor to evaluate the hoist systems at the U1a Complex. Tasks for the subcontractor include identifying components that require replacement to enhance operability or reliability and providing technical recommendations for improvements to components/systems. Given that the U1h hoist control system was not designed for a nuclear safety function, the staff team concludes that this would be an ideal opportunity to procure a system that is compliant with DOE directives and industry standards. This would allow MSTS to take credit for a greater risk reduction and improve assurance that the system will perform its intended safety function.

References

[1] Mission Support and Test Services, LLC, *U1a Complex Subcritical Experiments Documented Safety Analysis,* U1a-SCE-DSA-001, Revision 3, September 2019.

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

[3] Defense Nuclear Facilities Safety Board, *U1a Complex Safety Basis Review*, December 2018.

[4] Mission Support and Test Services, LLC, *Hoist Control System Overtravel PISA Report*, U1a-RPT-2019-020, Revision 1, January 2020.

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

[6] American National Standards Institute/International Society of Automation, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector,* ANSI/ISA 84.00.01-2004.

[7] Department of Energy, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities*, DOE Standard 1195-2011, April 2011.

[8] Mission Support and Test Services, LLC, *Statement of Work, Mission Support and Test Services, LLC, Time-and-Materials Architect Engineering Services Subcontract*, Solicitation Number: 352423-BZ-20, March 2020.

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

[10] 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.

[11] Thomas D. Barkand, *Emergency Braking Systems for Mine Hoists*, Proceedings of Symposium on New Technology in Mine Health and Safety, Subject Matter Expert Annual Meeting, Chapter 31, February 24–27, 1992.