DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Washington, DC 20004-2901

August 2, 2022

The Honorable Jennifer M. Granholm
Secretary of Energy
US Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Secretary Granholm:

The Defense Nuclear Facilities Safety Board (Board) has completed a review of the electrical systems supporting the Savannah River Tritium Enterprise (SRTE). The review assessed the safety and non-safety related electrical subsystems given their multiple points of interconnection. In addition, our staff reviewed numerous recent Occurrence Reporting and Processing System reportable events at the SRTE.

The enclosed report highlights the need for a systemic approach to aging management and health monitoring of safety significant systems and non-safety related electrical subsystems in the Tritium Enterprise. The enclosed report contains additional details and is consistent with Board Recommendation 2020-1 (Sub Recommendation 1.a): *"Develop and implement an integrated approach—including requirements—for the management of aging infrastructure that includes formal processes to identify and perform infrastructure upgrades necessary to ensure facilities and structures, systems, and components can perform their functions."*

Pursuant to 42 United States Code § 2286b(d), within 120 days, the Board requests a written report on SRTE's approach to system health monitoring for the safety significant glovebox oxygen monitors in its facilities.

Sincerely,

Joyce L. Connery
Chair

Enclosure

c: Mr. Joe Olencz

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Report

April 8, 2022

Savannah River Tritium Enterprise Electrical Review

Summary. The Defense Nuclear Facilities Safety Board's (Board) staff review team assessed the 13.8 KVAC and 480 VAC electrical distribution system supporting the Savannah River Tritium Enterprise (SRTE), focusing on design and equipment condition. The review was held over a series of teleconferences on March 16, 2021, and July 20, 2021. The review team's lines of inquiry (LOI) focused on both the safety and non-safety electrical subsystems because of their multiple points of interconnection and the inherent hazard that electrical systems represent to the workforce. In addition, the review team reviewed recent Occurrence Reporting and Processing System (ORPS) reportable events that have significantly impacted facility operation in the past five years. As a result of the COVID-19 pandemic, the review team did not perform onsite walkdowns of electrical equipment.

Background. The Tritium Extraction Facility (TEF) is located at the Savannah River Site. TEF's two primary missions are to receive and extract tritium, and to clean up extraction gases for transfer to H-Area New Manufacturing (HANM). The current mission for HANM is centered on gas separation, purification, and unloading and loading tritium reservoirs. Collectively, these facilities, along with others, are referred to as the Savannah River Tritium Enterprise (SRTE).

The staff review team conducted a detailed review of the following at SRTE:

- Electrical power systems,
- Instrumentation and control,
- Lightning protection system (LPS),
- Electrical calculations, and
- Procedures for response to loss of electrical power.

Discussion. Interactions between SRTE personnel and the staff review team were productive. The review team identified three key areas of concern: (1) the **lack of proactive response to the frequent glovebox oxygen monitoring instrument failures**, (2) the **lack of LPS maintenance**, and (3) **unvalidated electrical calculations**. The following sections discuss each of these concerns in detail.

Response to Recurring Equipment Failures—Many of the tritium processes take place in inerted gloveboxes to prevent a potential flammable gas mixture. Glovebox oxygen monitors are safety significant controls that alarm upon detection of elevated oxygen concentration to prevent fires and explosions having the potential to release tritium. Four types[1] of glovebox oxygen monitoring systems are used in the facilities reviewed. Regardless of the various configurations of the systems, the safety function of the glovebox oxygen monitoring systems for HANM and TEF is to ensure that the oxygen concentration in the glovebox confinement remains below the minimum level required to support combustion.

For more than a decade, the SRTE has experienced repeated failures in these systems (especially in HANM). In general, the failures are being identified and corrected during required periodic surveillances as the failures are typically not self-revealing (i.e., only found during surveillance). As a result of these repeated failures, the SRTE contractor is in the process of replacing the oxygen monitors in HANM. After 10 years, only 50 percent of the replacements have been achieved, and it is unclear when the project will be complete.

The technical safety requirements' (TSR) [1] specified surveillance frequency for the oxygen monitoring systems in HANM is every two months while the surveillance frequency is monthly for the systems in TEF. The documented safety analysis (DSA) specifies that the bases of these surveillance frequencies are "engineering judgment and operating history." When the review team inquired about the specific engineering judgement and operating history that justified a two-month surveillance for the oxygen monitoring systems in HANM and a monthly frequency for the oxygen monitoring systems in TEF, SRTE personnel indicated that the functional test frequencies are based on the following uncertainty evaluations:

- J-CLC-H-00920, for the Delta F system without the Panametrics;
- J-CLC-H-00929, for the Delta F system with a Panametrics;
- J-CLC-H-01053, for the Rosemount analyzer system; and
- J-CLC-H-00830, for the TEF Teledyne system.

The review team could not determine how the uncertainty evaluations could serve as the basis for the surveillance frequency difference between the facilities. Each uncertainty analysis listed the surveillance frequency (i.e., every two months or monthly) as an *input assumption* in the analysis; the effects of other surveillance frequencies were not subsequently evaluated. Given that the HANM oxygen monitors account for most of the documented failures discussed below, its less frequent surveillance (i.e., two months) is not technically justified particularly when compared to other oxygen monitors that have a monthly surveillance frequency.

The review team also evaluated ORPS for operational incidents related to oxygen monitors in the SRTE and noted repeated equipment failures in HANM. The SRTE contractor discovered failures of an audible alarm during surveillance testing of the P1-O2 oxygen monitor on 1/16/2018, 2/16/2018, and 4/16/2018 [2] [3] [4] and attributed each failure to the need to

[1] HANM uses three variations. The original design was based on a Delta F oxygen sensor inside the glovebox, a Delta F analyzer, and local credited alarms on the analyzer. The second variation uses a Delta F oxygen sensor, a Panametrics analyzer, and a local alarm panel that has the credited alarms. The third system in HANM is based on a Rosemount analyzer providing signals to a credited alarm panel located in the central control room. TEF uses only one style of glovebox oxygen monitoring system: a Teledyne system located inside the gloveboxes, a Panametrics analyzer outside the glovebox, a local alarm panel, and a credited control room alarm panel.

"reseat the alarm flasher module." These were preceded by audible alarm failures of the same oxygen monitor on 3/15/2016, 6/5/2017, 9/4/2017, 10/21/2017, 11/26/17, and 12/23/2017 [5] [6] [7] [8] [9] [10].

Based on the limited information available via ORPS, it appeared likely that the same failure mechanism was responsible for each of these failures. This failure mechanism appeared to be a mechanical issue with the alarm flasher module that had been corrected by simply reseating the module during troubleshooting activities. When asked if these ORPS reports triggered any additional evaluation of these events and if any corrective actions had been performed, the contractor, Savannah River Nuclear Solutions, LLC (SRNS), responded that these types of repeated failures were atypical for annunciator panels and likely stemmed from quality complications at manufacture. After the repeated failures, the project to replace the entire panel and system components was accelerated. The local alarm associated with the panel has now been replaced with a Central Control Room alarm.

The Unloading A Glove Box experienced an oxygen sensor failure on 5/29/2018 and experienced a second failure on 7/18/2018 [11] [12] even though the sensor had been replaced. Two failures within such a short period would typically indicate that an external influence caused the failures. When the review team inquired about these failures, SRNS responded that a 2009 analysis on the repeated oxygen monitor failures, SRNS-T0000-2009-00007, *Analysis of Tritium Facilities Glovebox Oxygen Monitor* [13], concluded:

> *[W]ith no discernable pattern or external influence, sensor failure could not be predicted. Until the new monitors are installed, failures in the oxygen monitors would continue, necessitating their reporting to National Nuclear Security Administration. The site does not perform formal predictive trending, but they have the ability to monitor O2 levels over time and can predict sensor failure due to drift by comparing sensor readings. However, the use of this data has sporadic validity as numerous monitors have failed without negative trending.*

After reviewing SNS-T0000-2009-00007 [13], the review team failed to identify data that would support this conclusion. The executive summary of SRNS-T0000-2009-00007 states:

> *Failure of the oxygen monitors appears to be related to a reduction in the diameter of the holes in the diffusion barrier, an integral part of the sensor. These holes allow the passage of sample gas (containing oxygen) to the electrode of the measurement cell. The reduction in size is due to the collection of particles in and around the entrances of the holes probably due to tritium induced degradation of the diffusion barrier.*
>
> *Since the failure appears to be primarily a narrowing of the diffusion barrier holes which can only be observed via destructive examination, there is no realistic or reliable way of predicting when the cells will fail. Therefore, a replacement type of oxygen monitor needs to be identified and tested. Until the new monitors are installed, failures in oxygen monitors will continue necessitating their reporting to NNSA [National Nuclear Security Administration].*

The report also identified the following:

A six-sigma analysis was performed to identify correlations between individual and groups of monitor failures. This analysis looked for common trends between failures, such as which stripper system was associated with the failing monitors, glovebox activity, monitor age, etc. No common trends between failed monitors were discovered during this analysis. However, the results determined that, on average, cells fail approximately every 35 months.

The report concluded with the following recommendation:

The purpose of the Tritium Facilities HANM glovebox oxygen monitor analysis was to determine why the monitors were failing more often than expected. An understanding of the mode for failure was the first step in being able to predict failure and identify a possible remedy to prevent future failures and extend the life of the monitor. The analysis showed that the primary mode of failure (reduction in diffusion barrier hole diameter) can not be readily detected or corrected, and that prediction of monitor failure and extending the life of a monitor are impractical with the current oxygen monitors.

Due to the age of this particular oxygen monitor technology, and development of new technologies, and the complexity of the mode of failure, it is recommended that new alternatives to measure glovebox oxygen be identified and researched. Alternatives should be tested in a tritium environment prior to being incorporated to determine the effect of tritium on the monitors. In the meantime, a cost benefit analysis is being performed to determine the optimum frequency of replacement of the current monitors to maximize use and minimize failure and cost. This cost benefit analysis incorporates the results of the six sigma analysis performed as part of this testing phase.

The review team found no evidence that engineering personnel used this 2009 analysis to actively improve the reliability of the existing oxygen monitors. On the contrary, SRNS personnel cited the analysis as a justification that oxygen monitor failures could not be predicted even though the analysis concluded that "…the results determined that, on average, cells fail approximately every 35 months." However, this information did not appear to be used as a basis for determining any type of maintenance activity or replacement schedule. Based on this, the review team observed that a philosophy of *operate until failure* is the prevailing strategy for component replacement.

As noted above, SRNS personnel informed the review team that they have replaced roughly 50 percent of the oxygen monitors in HANM and would continue to monitor sensor failures until the project is complete. On average, SRNS has annually replaced one to two monitors. While there is indication that the replacement rate will increase in future years, it has already been more than a decade since facility personnel identified problems associated with the HANM glovebox oxygen monitoring system, and it is unclear when the project will be complete.

The evaluation of the reliability of the new sensors remains weak. When asked to discuss the performance of the new monitors, SRNS engineering personnel said that they do not actively track individual sensor failures and do not have any readily available information to determine if the new sensors have corrected the previously identified problem. Given the sporadic nature of the data currently available, a documented analysis is needed to evaluate whether the performance of the replacement sensors is free from dormant failures and assess whether the current surveillance and replacement strategy is adequate. It would be appropriate for SRTE to use a system health monitoring approach that focuses on system availability with a targeted acceptability level (e.g., 98 percent). For reference, the nuclear industry has developed well-supported approaches to conducting aging and simulated environmental testing to detect aging and environmental degradation with Institute of Electrical and Electronics Engineers (IEEE) Standard 323, *Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, and related quality assurance standards.

In summary, ensuring the reliability of safety systems is one of the most important aspects of system design. For example, 10 Code of Federal Regulations (CFR) 830.122(c) Criterion 3, *Management/Quality Improvement*, states, "Identify the causes of problems and work to prevent recurrence as a part of correcting the problem." While SRNS's 2009 analysis concluded that sensor replacement was the only viable strategy to correct the concern, the rate of replacement has clearly been too slow to prevent recurrence of failures. In addition, the new oxygen monitors are almost certainly more reliable than the older models, but SRNS personnel were unable to provide documentation demonstrating their improved performance. Without such an analysis, it is difficult to conclude that the original problem with the oxygen monitors has been adequately addressed and the reliability of these replaced safety system components has been demonstrated.

Lightning Protection Systems Have Not Been Maintained—Lightning is a known hazard to facilities at the Savannah River Site. As documented in Section 1.5.5 of the TEF DSA [14], "Lightning is a normal occurrence on site and is considered an accident event initiator in the hazard analysis." Lightning strikes present a number of hazards to nuclear facilities, but the most commonly analyzed are the ignition of fires and impact to electrical equipment. The guidelines in Annex L of National Fire Protection Association (NFPA) 780, *Standard for the Installation of Lightning Protection Systems* [15], are typically used to determine whether specific facilities subsequently require lightning protection.

According to the facility safety bases, TEF [16] and HANM [17] are each equipped with an individual LPS originally installed per NFPA 780. Lightning is analyzed in both documents as an accident initiator, primarily fire, with the LPSs discussed further in the facility *Fire Hazard Analyses*. In addition, the TEF electrical power supply system design description [18] goes on to capture the following requirement (R.EPSS.7.2.4), "The lightning protection system shall minimize the damage to equipment, and shall meet the requirements of NFPA-780 and NFPA 70, *National Electrical Code* [19]."

Based on the documents above, the review team included several LOIs to assess the status of the LPSs installed on SRTE facilities. In response, SRNS stated that the LPSs are not credited controls in the SRTE safety bases and therefore are not being actively maintained per NFPA 780. As such, there does not appear to be current information on the status of LPS equipment or the adequacy of its coverage. While it is true that the LPSs are not credited structures, systems, or components (SSCs), they still perform an important safety function when properly installed and maintained.

Conversely, an improperly installed and maintained system will continue to attract lightning strikes but may no longer be able to safety redirect that energy away from the facility and its credited SSCs. As SRNS engineering personnel were unable to answer questions about the system's current configuration and nominal coverage areas, the review team does not have sufficient information to determine the potential impact of the LPSs' current condition. Since the functionality of the LPSs is indeterminate, the hazard lightning can present to the facility and credited electrical SSCs (e.g., uninterruptible power supply [UPS]), glovebox oxygen monitoring system) is unknown. The current LPSs likely no longer meet the requirements of NFPA 780, and their condition represents a potentially substantial degradation to an important defense-in-depth system. In the worst case, extreme deficiencies could lead to the facility operating outside its DSA as the safety basis and credited SSCs assume that a functional LPS will reduce the consequences of lightning strikes.

In response to the review team's concerns, SRNS undertook a gap analysis on the SRTE LPSs. The review team requested NNSA to provide the gap analysis for review.

The Electrical System Model Is Not Validated with Field Measurements—ETAP is the most common electrical power system modeling software used in the nuclear industry. It is used for a variety of electrical system calculations such as load flow, electrical protection device coordination, and transient analysis. The ETAP software package is popular in the nuclear industry for several reasons, the most important being the robustness of its quality assurance program (e.g., compliance with American Society of Mechanical Engineers *Nuclear Quality Assurance* (NQA)-1 and 10 CFR 50 Appendix B, *Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants*). However, like any computer software package, the fidelity of its calculations is only as good as the accuracy of its inputs.

The facility's electrical design details (e.g., cable lengths, load type, protection devices, ratings of equipment) must be manually entered into the software to reflect their installed configuration in the facility. The accuracy of these entries is typically supported by comparison with facility electrical one-line drawings and field walkdowns, both of which SRNS personnel communicated were performed for the SRTE. However, one additional validation is necessary to ensure that the electrical model's calculations adequately reflect the performance of the electrical system: a comparison of at least some steady-state calculated values with field measurements. The simplest such comparison would be an assessment of the voltage predicted by the software compared against actual system voltage measurements, ideally taken at voltage limiting components and critical load terminals.

The electrical grid typically maintains nominal, or higher, system voltage, but weather conditions, electrical faults, etc., can degrade the voltage to 80 percent of nominal or lower. To ensure the safety function of electrical equipment, it is important to know the voltage band within which all required equipment can perform its function. The most vulnerable equipment includes electrical contactors, dampers, and solenoid-operated equipment (e.g., used for confinement, tripping, starting) that could become inoperable under reduced voltages. The operability of such safety-related components, located further away from power sources, cannot be reasonably assured under the full anticipated spectrum of operating voltages without a field-validated software model. Unfortunately, such a vulnerability and its potential impact will remain unknown until a reduced voltage condition is present.

An electrical grid voltage degradation event in the early 1970s caused automatic and manual control failures for safety systems in the nuclear power industry. Based on the level of voltage degradation, the plant impact could have wide and indeterminant variation. A significant voltage drop could lead to increased current draw for most loads and could result in several common cause failures (e.g., opening breakers, blowing control circuit fuses). Multiple failures over a limited time could result in unanticipated equipment performance. In addition, operator response to such problems could further be challenged by the loss of automatic and/or manual actions. The Nuclear Regulatory Commission (NRC) has been addressing the adequacy of utility voltages since the late 1970s (e.g., NRC Generic Letter 79-36, Info. Notices 79-04, Regulatory Issue Summary 2000-24) and is a source for information, examples, and/or requirements for preserving adequate voltage under all anticipated operating conditions to support safety system performance.

In response to the review team's concerns, SRNS communicated that it considers the quality assurance program of the ETAP modeling software developer, combined with the SRNS quality assurance program on the verification of loads, to be adequate. Therefore, SRNS does not consider field validation of the software voltage calculations to be necessary. The staff team noted, however, that the vendor's quality assurance is limited to fidelity of the calculations performed by the modeling software. The software does not include any verification of installed cable lengths, actual contact resistances, and potential degradations at terminations, which are unique to the specific installation.

An unvalidated software model may obscure significant problems that only become apparent when an adverse event takes place. Given the lessons learned by the larger nuclear industry, NNSA and SRNS should consider adding a simple validation of predicted versus actual voltages in the field to better ensure that equipment important to safety will perform as required under all anticipated electrical grid operating conditions.

Additional Observations. In other areas evaluated by the review team, site personnel demonstrated a healthy questioning attitude, sound technical judgment, and a commitment to appropriate maintenance practices. Other observations the review team communicated to SRTE personnel are summarized below.

Loss of Electrical Power—The review team discussed entry into HANM's abnormal operating procedures for response to loss of power in the facility. The team believes the qualifier to "evaluate" entering the limiting conditions for operation (LCO) without specific criteria could be confusing and lead to inconsistent applications. For example, upon loss of power, the expectation is that the LCOs for the HANM tritium air monitoring and glovebox oxygen monitoring systems will be entered immediately. In contrast, the LCOs for the HANM enclosure oxygen monitoring systems in the environmental conditioning enclosure and the environmental conditioning room electrical isolation system would only need to be entered upon loss of power if the systems are in operation. For the HANM tritium air monitoring and glovebox oxygen monitoring systems, direction to "enter" the LCO as opposed to the current "evaluate entering" would be consistent with the abnormal operating procedures for these same systems in TEF, where the expectation is to always enter the LCOs upon loss of power. Clearer language would improve operators' ability to respond to this abnormal condition.

Underground Power Cable Monitoring—The SRTE is supported by a combination of above and below ground electrical power distribution cabling. The underground cabling is predominantly direct burial. The current management strategy for this aging equipment is to procure spare long-lead-time cabling, as needed, and operate the existing buried equipment until replacement is necessary. Current maintenance operations do not include a condition monitoring program for underground cables and connectors to assess/trend the level of degradation from aging or other environmental factors. The review team communicated that a maintenance program that includes condition monitoring for cables and connectors is recommended when relying on underground power cabling as simpler techniques (e.g., visual inspection) are not always practical. When one degraded cable fails, the resulting voltage transient could fail other cables that are near failure in the same distribution system. Such incidents could make power recovery extremely time consuming. Adequately maintaining distribution cabling can prevent in-service failures and protect personnel and equipment from electrical shock, arc flashes, and excessive electrical currents.

Tritium Air Monitors—During discussions with SRTE personnel, the review team inquired about the health of the tritium air monitors as reported in issued system health reports since May 2016. Based on evidence provided to the review team over two teleconferences and the responses to the team's lines of inquiry, SRTE personnel demonstrated they have the appropriate technical expertise and skill set to deal with ongoing issues resulting from aging and obsolete components for this equipment.

Conclusion. Based on the review team's observations, SRNS engineering personnel appear to have normalized deviations and component failures of the safety significant glovebox oxygen monitors. This apparent lack of a questioning attitude extends to the performance of maintenance on the LPS and validation of calculated values from the ETAP model with field measurements. Facility safety equipment performance could be improved by facility personnel proactively responding to component failures, addressing the direct and indirect root causes of such failures, and demonstrating that the equipment qualification program adequately simulates aging and worst-case environmental conditions (proof testing) before installing new safety equipment in service. In addition, facility personnel could enhance LPS performance by performing recommended preventive maintenance and correcting any deviations/degradations discovered by the gap analysis. Finally, facility personnel could better demonstrate the adequacy of the existing facility electrical distribution system by validating the power system engineering calculations with field measurements.

References

[1] SRNS, "Technical Safety Requirements Savannah River Site Tritium Facilities," WSRC-TS-96-17-1, Rev. 31, October 2020.

[2] "ORPS: SRSO-SRNS-TRIT-2018-0003."

[3] "ORPS: SRSO-SRNS-TRIT-2018-0006."

[4] "ORPS: SRSO-SRNS-TRIT-2018-0011."

[5] "ORPS: SRSO-SRNS-TRIT-2016- 0004."

[6] "ORPS: SRSO-SRNS-TRIT 2017-0009."

[7] "ORPS: SRSO-SRNS-TRIT 2017-0012."

[8] "ORPS: SRSO-SRNS-TRIT 2017-0013."

[9] "ORPS: SRSO-SRNS-TRIT 2017-0014."

[10] "ORPS: SRSO-SRNS-TRIT 2018-0001."

[11] "ORPS: SRSO-SRNS-TRIT-2018-0013."

[12] "ORPS: SRSO-SRNS-TRIT-2018-0015."

[13] P.J. Foster, J.R. Quarles, R.E. Snyder, R.A. Malstrom, L.L. Tovo, "Analysis of Tritium Facilities Glovebox Oxygen Monitors," SRNS-RP-2008-01338 rev 0, 2009.

[14] SRNS, "Tritium Facility Documented Safety Analysis," U-DSA-H-0002 Rev 0, 2017.

[15] National Fire Protection Association, NPFA 780, "Standard for the Installation of Lightning Protection Systems," 2008.

[16] SRNS, "Tritium Extraction Facility Safety Analysis Report," WSRC-SA-1-2-VOL-4, Rev. 14, 2020.

[17] SRNS, "Tritium Facilities Safety Analysis Report," WSRC-SA-1-2-VOL-1, Rev. 26, 2020.

[18] SRNS, "TEF System Design Description for Electrical Power Supply Systems," E-SYD-H-00001, Rev. 10, 2015.

[19] National Fire Protection Association, NFPA 70, "National Electrical Code," 2017.

[20] SRNS, "Tritium Facility Technical Safety Requirements," U-TSR-H-00004, Rev. 0, 2010.

[21] NRC, "Information Notice No. 79-04, Degradation of Engineered Safety Features," 1979.

[22] NRC, “Generic Letter 79-36: Adequacy of Station Electric Distribution Systems Voltages,” 1979.

[23] NRC, “RIS: Concerns About Offsite Power Voltage Inadequacies and Grid Reliability Challenges Due To Industry Deregulation,” 2000.