Received by the Board 12.20.22

Department of Energy
Under Secretary for Nuclear Security
Administrator, National Nuclear Security Administration
Washington, DC 20585

December 19, 2022

The Honorable Joyce L. Connery
Chair, Defense Nuclear Facilities Safety Board
625 Indiana Avenue NW, Suite 700
Washington, DC 20004

Dear Chair Connery:

The Department of Energy's National Nuclear Security Administration (DOE/NNSA) received your letter, dated August 2, 2022, regarding the Savannah River Tritium Enterprise (SRTE) approach to system health monitoring for the safety significant glovebox oxygen monitors in its facilities. I am responding on behalf of the Secretary of Energy. The letter established a 120-day reporting requirement to address DOE/NNSA's approach.

NNSA remains committed to strong and effective safety systems at SRTE. The current approach demonstrates that assessing system health using component utilization provides a reliable indicator of system performance. Enclosed is SRTE's report, J-ESR-H-00138 – SRTE System Health Reporting Program, that presents data and conclusions regarding the glovebox oxygen monitoring systems and supports the upgrades in the H-Area New Manufacturing Facility.

If you have any questions, please contact Mr. Jason Armstrong, Savannah River Field Office Manager, at (803) 208-3689.

Sincerely,

Jill Hruby

Enclosure

Received by the Board 12.20.22

Received by the Board 12.20.22

J-ESR-H-00138

SRTE System Health Reporting Program

Prepared by:	M. E. Farrar M. E. Farrar, SRTE Electrical Engineering	11/29/2022 Date
Reviewer:	J. W. Ingold, SRTE Design Authority Engineer	11/29/2022 Date
Revision No:	2	
Revision Date:	11/29/2022	

APPROVAL SIGNATURES

Approved by:	S. J. Mazurek, Manager, Project Design Authority & Regulatory Programs	11/29/2022 Date
Approved by:	K. G. Aylward, SRTE Deputy Chief Engineer	11/29/2022 Date

DOES NOT CONTAIN UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

Reviewing Official/Denying Official: Joel Ingold, JWI, SRTE Engr
(Name/Organization)

Date: 11/29/2022

Received by the Board 12.20.22

Received by the Board 12.20.22

ABSTRACT

The Defense Nuclear Facility Safety Board has expressed concerns with Safety Significant equipment and reliability in SRTE facilities. The DNFSB concluded there is a "need for a systemic approach to aging management and health monitoring of safety significant systems and non-safety related electrical systems in the Tritium Enterprise." This report is in response to the data presented and conclusions drawn regarding the Safety Significant Glovebox O_2 Monitoring Systems in SRTE.

SRTE is actively engaged in a robust system health monitoring program that is in compliance with the SRS Conduct of Engineering manual E7 procedure 3.04. Data from the Glovebox O_2 Monitoring system health reports for the past three reporting periods are presented that demonstrates how the Design Authority engineer trends equipment reliability, as defined by corrective maintenance activities performed, to trend systemic problems at the component level. This report demonstrates how trending equipment reliability provides a more reliable and leading indicator of system performance than system availability and discusses how analysis of equipment failures at SRTE leads to design changes to resolve performance problems. A recent example of repetitive failures in the Glovebox O_2 Monitoring system is used to demonstrate how the process proceeds to a resolution. This process includes troubleshooting to isolate the failure mechanism, analysis to determine the best path forward, and, potentially, design for facility modifications. The process is deliberate to ensure the safety function of the system is not compromised. In addition, the complexity of the implementation process is discussed.

Overview of System Health Monitoring for Glovebox O_2 Monitors

Each Design Authority Engineer (DAE) is responsible for monitoring activities related to their systems on a daily basis. There are multiple systems and processes used every day in the facility that either require DAE approval or provide the DAE with insight into facility activities. For instance, the work control process ensures that all non-routine work packages for SS systems are reviewed and approved by the DAE. Similarly, DAE's have access to the Shift Technical Engineer's (STE) log which informs them of critical activities and evolutions that have occurred in the facility. DAE's are encouraged to be in the facilities regularly to interface with Operations, Shift Technical Engineering, and Maintenance personnel to collaboratively discuss and review conditions and concerns as they occur so that trends can be identified, and discrepant conditions resolved.

STE's review daily functionals for the O_2 monitors as well as the O_2 monitor roundsheets. In addition, they regularly review trend data for specific equipment and systems to identify abnormalities. Suspect data is communicated to the appropriate DAE for review and action. For instance, STE's compare Glovebox O2 monitor readings to process conditions to evaluate whether the monitor readings are suspect. A review of LCO data in 233-H shows that this simple review identified 67% of the cell failures recorded from the period 3/1/2019 – 2/28/2022. While neither the Delta F nor the Panametrics instruments have the capability to diagnose and communicate cell failures and are therefore not "self-revealing", a simple evaluation based on process knowledge effectively identifies most cell failures.

Moreover, Engineering has been collecting and trending surveillance data on the Glovebox O_2 Monitors since 2005 in HANM and 2007 in TEF. Engineering uses this data to identify monitor locations exhibiting long term instabilities and location specific failures. This data has been invaluable with the new Rosemount XEXF analyzers because the surveillance data shows that some instruments require periodic

Received by the Board 12.20.22

Received by the Board 12.20.22

optimization to maintain calibration. This has resulted in Engineering taking action to contact the vendor and evaluate potential mechanisms for this behavior as well as identify probable solutions.

SRTE System Health Reporting for Glovebox O_2 Monitoring

SRTE has a robust system health monitoring program in accordance with the SRS Conduct of Engineering manual E7 procedure 3.04, which is in compliance with 10 CFR 830.122. SRTE management, (Operations, Engineering, Maintenance, and Projects), holds regular meetings in which systems are presented by the respective Design Authority engineers on a rotating basis to ensure every system is reviewed by management annually. Each Design Authority engineer is responsible to "select the appropriate parameters to monitor and...initiate the appropriate actions to implement the monitoring activities." In the case of Glovebox O2 Monitoring in HANM, the primary parameter tracked by the DAE is the number of component replacements. As an example, Tables 1 - 3 were taken from the last three system health reports. These tables show the components that were replaced and demonstrate the improvement in reliability achieved through replacing the Delta F oxygen monitors. For reference, the reporting period for each table is March 1st of the previous year to February 28th of the next year.

Table 1: HANM Glovebox O_2 Monitor Corrective Maintenance, 2020 Reporting Year

Delta F Component Replacements (26 Instrument Locations)	Rosemount Component Replacements (9 Instrument Locations)
24 Delta F O_2 Cell	2 Pump
1 Delta F Main Board	2 Analyzer
2 Power Supply	6 Ronan Alarm Card
1 Delta F Flow Board	
2 Chemtec Flow Switch	
1 Pump	
1 Dwyer Rotameter	
1 Terminal Strip	

Table 2: HANM Glovebox O_2 Monitor Corrective Maintenance, 2021 Reporting Year

Delta F Component Replacements (19 Instrument Locations)	Rosemount Component Replacements (16 Instrument Locations)
22 Delta F O_2 Cell	1 Pump
2 Delta F Main Board	1 Metering Valve
1 Delta F Flow Board	1 Analyzer
3 Chemtec Flow Switch	5 Ronan Alarm Card
2 Pump	
2 Dwyer Rotameter	
2 Sample Line Tubing	

Received by the Board 12.20.22

Received by the Board 12.20.22

Table 3: HANM Glovebox O_2 Monitor Corrective Maintenance, 2022 Reporting Year

Delta F Component Replacements (14 Instrument Locations)	Rosemount Component Replacements (21 Instrument Locations)
15 Delta F O_2 Cell	2 Pump
3 Delta F Main Board	1 DCS card
1 Delta F Display	2 Cell
1 Power Supply	7 Ronan Alarm Card
3 Delta F Flow Board	
1 Annunciator module	

For comparison, the TEF component replacements are shown in Table 4. The DAE for the TEF Glovebox O_2 Monitoring system does not typically report this data in the System Health Report, because the system is stable and does not currently exhibit a preferred failure mode. Therefore, a more representative metric is the cost of corrective maintenance. However, the data presented in Tables 1 – 4 is readily available in the Tritium Work Management System (TWMS) database and can easily be trended by the DAE when an unusual pattern, such as repetitive CM at a specific location or increased incidence of a specific failure mechanism, is detected. The DAE may identify those cases during their review and approval of the work packages or Operations may request a review based on process experience.

Table 4: TEF Glovebox O_2 Monitor Corrective Maintenance, Reporting Years 2020 – 2022

Component Replacements (9 Instrument Locations)	2020	2021	2022
Pump	1		1
Display Card	1	1	
Front Panel Display	1		
Fuse			2
Power Supply Card			1
Analyzer			1

Evaluation of Replacement Oxygen Monitors in HANM

By breaking the HANM corrective maintenance down to the component level, emphasis is placed on the high number of oxygen cell failures as a reminder of the urgency to replace the remainder of the Delta F instruments. The data from the tables is compiled in Figure 1 for all three years and then normalized to the number of installed instruments in Figure 2. This demonstrates how the Delta F corrective maintenance is directly proportional to the number of Delta F instruments in service. While not normally used in the system health evaluation, these figures are provided here to illustrate the impact of replacing the Delta F O_2 sensors.

Received by the Board 12.20.22

Received by the Board 12.20.22

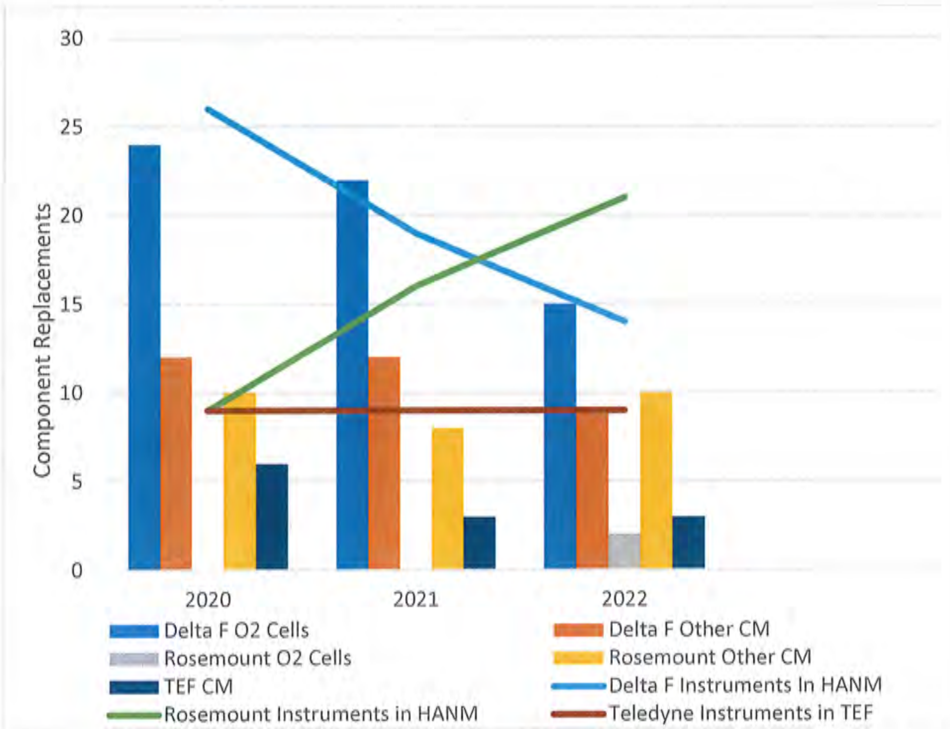

Figure 1: Tritium Facilities Glovebox O_2 Monitor Corrective Maintenance by Year

The impact of replacing the HANM Glovebox O_2 Monitors with the Rosemount XEXF was immediate and obvious. As illustrated in Figure 1, the replacement of Delta F O_2 sensors is directly correlated to the number of instruments in the field that are using those sensors. A documented analysis has not been performed to date on the Rosemount analyzers because of the positive impact of installing the new equipment. The relatively few problems that have been identified with the new equipment are being addressed as a result of the existing processes and systems as described here. As discussed previously, the DAE has identified that certain instruments require periodic calibration adjustment as a result of the surveillance data trending that is performed. Because the DAE tracks component replacement as an indicator of reliability instead of tracking availability, the alarm panel associated with the new Rosemount analyzers has been identified as a reliability impact, and actions are being taken to redesign alarm annunciation.

Received by the Board 12.20.22

Received by the Board 12.20.22

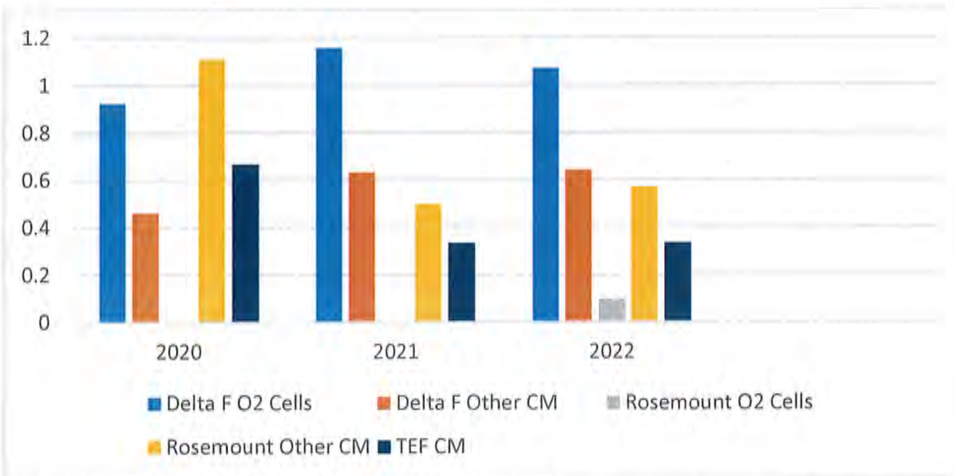

Figure 2: O_2 Monitor Corrective Maintenance Normalized to the Installed Instrument Base.

Aging and Environmental Degradation Testing

IEEE 60780-323-2016 specifies, "A qualified life is not required for equipment located in a mild environment and which has no significant aging mechanisms and is operated within the limits established by applicable specifications and standards." A mild environment is defined as an "environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences". During the design phase, Engineering developed a specification which included all technical requirements for the new equipment based on the safety function, Safety Basis-related requirements, and environmental conditions. During the testing phase, the equipment was tested to demonstrate it met the requirements of the Engineering specification as well as the relevant manufacturer's specifications. Additional aging and simulated environmental testing is neither required nor appropriate since this equipment operates in a mild environment and is not required to be operational during or after a Design Basis Event.

Repetitive Failures

By normalizing the corrective maintenance to the number of instruments installed, it becomes clear that, while the Rosemount analyzers have a more reliable oxygen cell, there have been some routine equipment failures. Referencing Tables 1 - 3 again, it is noted that the alarm panel installed for the new Rosemount analyzers has experienced an excessive number of alarm card failures. This is not the same alarm panel addressed in DNSFB Staff Report dated April 8, 2022. This is a newer panel that was installed in the control room to service alarms from the Rosemount analyzers. However, the process by which repetitive failures occur before the issue is identified and resolved is similar.

The P1-O2 alarm panel failures referenced by the DNSFB are a clear example of this process in action. The alarm panel in question is of a type in general use in the nuclear industry. Each alarm flasher module plugs into the backplane of the alarm panel using card edge connectors. These connections are rugged and reliable but can be subject to intermittent behavior. The primary failure mode is loss of conductivity but the mechanism for losing conductivity can be varied. A common mechanism is build-up on the

Received by the Board 12.20.22

Received by the Board 12.20.22

connector edge. Therefore, a primary troubleshooting technique is to unseat and reseat the connector, effectively wiping the card edge clean. If the problem is recurring, then other actions will be taken to identify or correct the problem. The scenario, then, is that the alarm flasher module is removed to perform diagnostic and potentially corrective maintenance such as verifying continuity, visual inspection for damage or corrosion, tightening of screws on terminal strips, or other similar actions. When all the planned actions have been taken the alarm flasher module is reseated and is found to be working. At that point several actions have been taken but it may be indeterminate which one corrected the problem. In any case, troubleshooting cannot continue because the symptoms are no longer apparent; therefore, the Post Maintenance Test (PMT) will be performed to determine if there are any other indications of failure. If the PMT is successful, then the system will be returned to Operations because it has demonstrated its ability to perform the safety function. In the ORPS report, the action taken to return the system to service is identified as "reseat the alarm flasher module" because the actions taken prior to inserting the alarm flasher module are considered diagnostic in nature or cannot be confirmed to have solved the problem. In this case, the problem was eventually identified as misalignment between the alarm flasher module and the panel backplane and actions were initiated to modify the design and remove the panel from service. Because the panel and module did not exhibit any wear or damage and the components met the manufacturer's specifications, the problem was attributed to dimensional tolerancing. For this reason and others, it was determined that the most efficacious path forward was to modify the design to remove the alarm panel entirely. The DAE's informal evaluation of extent of condition did not indicate a history of this type of failure in the tritium facilities.

Always, when performing maintenance, the goal is to return the system to safe operation as soon as possible. If Maintenance performs corrective maintenance which they believe has resolved the issue and the DAE-specified Post Maintenance Test demonstrates the system can perform its safety function, then the system will be returned to service. Repetitive failures are not a desired occurrence, but there are times when there may be multiple potential failure mechanisms which must be tested serially to determine the failure mechanism, and multiple failures can occur before the problem is resolved. That level of detail is not available in the ORPS report because that is not the purpose of the report.

Delta F Failure Analysis

In 2008 SRTE requested a failure analysis be performed on the Delta F Oxygen cells due to an unacceptably high replacement rate. The failure analysis report, SRNS-T0000-2009-00007, concluded the primary failure mechanism was due to degradation of the diffusion barrier probably caused by tritium decay. The study also concluded that there was not a reliable way to predict failure or monitor degradation. A six sigma analysis was performed in conjunction with the failure analysis to identify statistically significant correlations in cell failure rates and locations in the facility or significant changes in the failure rate over time. No statistically significant correlations were found. The executive summary clearly states, "...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..." SRTE used this information to immediately begin a search for a more reliable oxygen monitor.

Received by the Board 12.20.22

Received by the Board 12.20.22

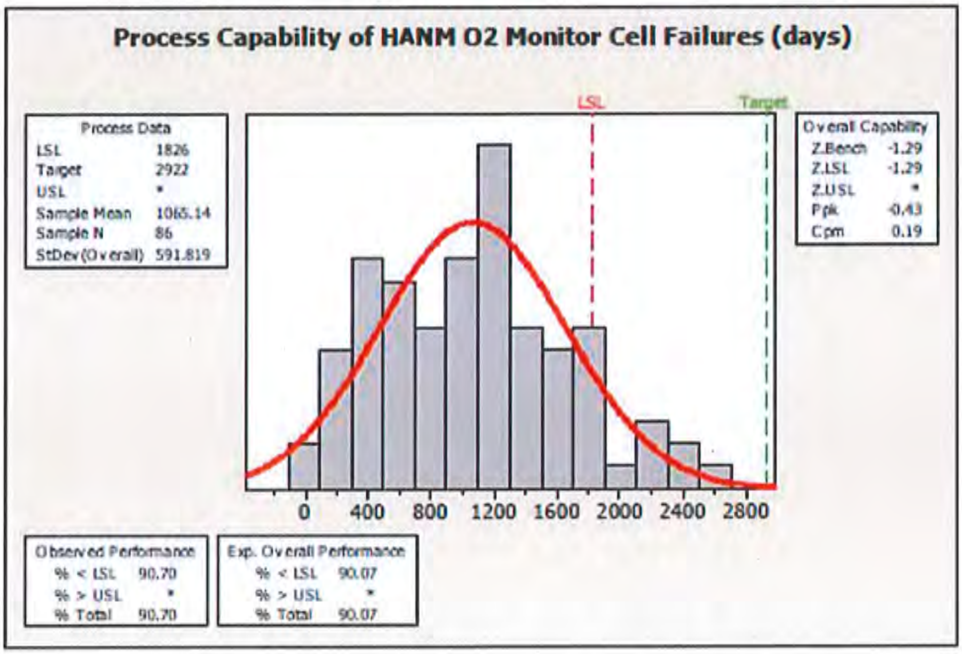

Figure 3: Mean Time To Failure for Delta F Oxygen Sensors

Although the study clearly states there is no reliable way to predict failure, the DNFSB report implies that a maintenance activity or replacement schedule should have been implemented based on this study. The report quotes a summary statement of the six sigma analysis that states, "on average, cells fail approximately every 35 months" as the basis for that assertion. The data requires a more nuanced evaluation than a simple average Mean Time To Failure (MTTF). Chart 6 from the six sigma analysis is reproduced above as Figure 3. In the Figure, the Mean Time to Failure data for the cells used in the analysis are plotted. The plot demonstrates a wide variability in MTTF with a significant skew towards early failure. Because the standard deviation is excessive, early failure is highly probable, and failure is unpredictable, the DAE determined there was a high likelihood that a strategy of scheduled cell replacement would induce a higher rate of equipment outages. As a result, a run to failure strategy was chosen to ensure the highest reliability possible until the equipment could be replaced.

System Availability and Reliability

Availability for SS systems can best be calculated based on the percentage of time spent in unplanned LCO's. Figure 4 and Figure 5 show the availability of each oxygen monitor location in HANM and TEF, respectively, for the reporting period of 3/1/2021 – 2/28/2022, which corresponds with the 2022 System Health Report period. Based solely on availability, it would appear that only two instruments were available less than 98%, but the majority have availability greater than 98 % in HANM. The focus, then, would be on the two instruments with low availability. In fact, however, an analysis of each unplanned LCO reveals that the low availability was due to those instruments being in one or more extended outages while diagnostic activities were carried out by engineering and maintenance. Similarly, the two instruments in TEF that fell below 98% did so because of a single extended corrective maintenance activity. If system availability, then, was the primary indicator of operational performance,

Received by the Board 12.20.22

Received by the Board 12.20.22

focus would be skewed to events representing unique failures and long term, repetitive, issues would be masked. Masking of repetitive corrective maintenance activities occurs because maintenance makes a concerted effort to ensure adequate levels of critical spare parts are always on hand and engineering invests significant resources in mentoring and educating maintenance personnel one on one in the field. This results in most corrective maintenance activities requiring less than 48 hours to diagnose and repair. Therefore, availability tends to be a lagging indicator and masks true repetitive corrective maintenance issues requiring engineering attention to resolve.

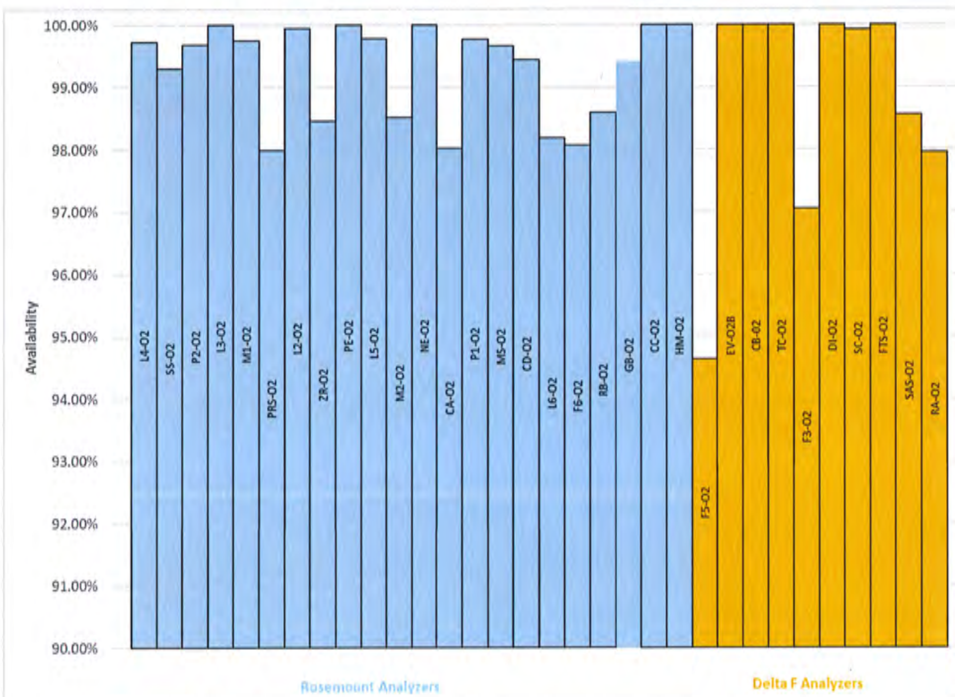

Figure 4: HANM Glovebox O_2 Monitor Availability*

*Availability defined as percentage of time not in an unplanned LCO. LCO's entered due to planned surveillance or preventive maintenance are not included.

Received by the Board 12.20.22

Received by the Board 12.20.22

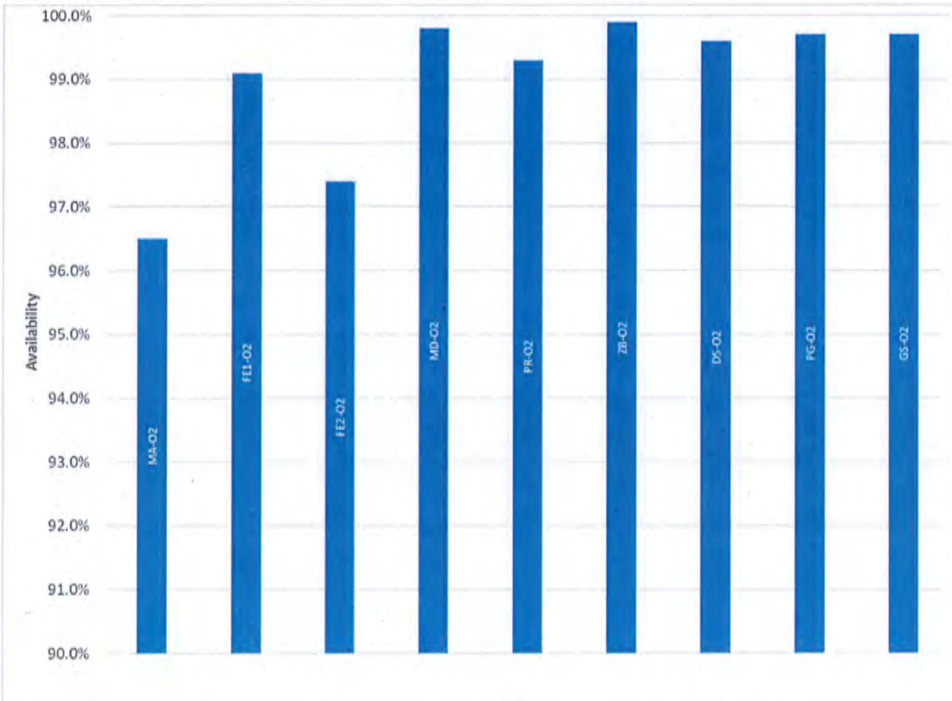

Figure 5: TEF Glovebox O_2 Monitor Availability*

*Availability defined as percentage of time not in an unplanned LCO. LCO's entered due to planned surveillance or preventive maintenance are not included.

Similarly, while the corrective maintenance data presented in Tables 1 - 3 clearly demonstrate a major impact on operational reliability is being corrected by upgrading the instruments in HANM, it also shows a new operational risk was introduced with the new alarm panel. But, neither historical trending of LCO data nor ORPS reportable events, as shown in Figure 6, reflect those realities.

Received by the Board 12.20.22

Received by the Board 12.20.22

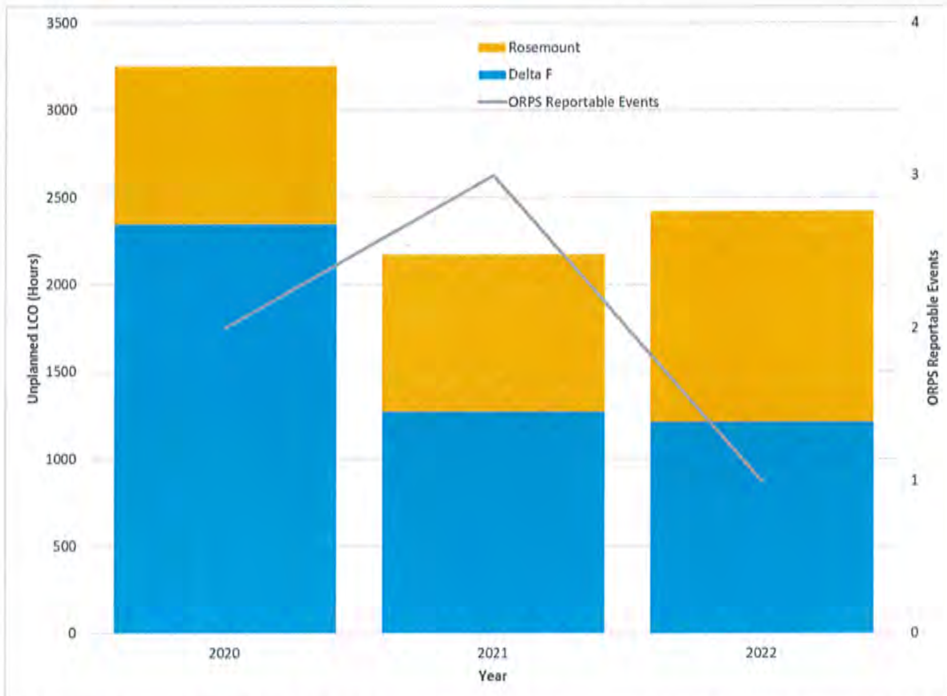

Figure 6: Historical Trend of HANM Corrective Maintenance and ORPS Reportable Events

Technical Basis for Surveillance Frequency

As pointed out by the DNSFB, the safety analysis specifies that surveillance frequency is based on engineering judgement and operating history. It is the DNFSB's judgement that the HANM oxygen monitor surveillance frequency of 60 days "is not technically justified particularly when compared to other oxygen monitors that have a monthly surveillance frequency." The surveillance frequency for the TEF oxygen monitors was defined during startup of that facility. When equipment lacks an extensive operating history to justify a longer frequency, 30 days is considered normative. Because the TEF system is a small system and has performed satisfactorily, a 60 day surveillance frequency would be justified; however, there has been no safety, operational, or financial incentive to adjust the surveillance frequency. Therefore, reducing the surveillance frequency of the HANM oxygen monitors to 30 days because TEF is at 30 days is not adequate technical justification.

SRTE agrees that the Delta F oxygen monitors have a known failure mechanism in the O_2 cell. Because of that known failure mechanism, SRTE has invested in a replacement program that has proven to have a positive impact on the number of corrective action events. Moreover, when system availability is assessed, 7 of the 9 oxygen monitors in TEF and 33 of the 35 oxygen monitors in HANM meet or exceed 98% availability in the latest reporting period. In addition, all the monitors were above 94% availability. This points to SRTE's assertion that the problem is being managed effectively and a run to failure strategy for Delta F cell maintenance is limiting the impact to system availability. Availability is expected to continue to improve as the remaining Delta F oxygen monitors are replaced; therefore, there is no technical justification to reduce the surveillance frequency.

Received by the Board 12.20.22

Received by the Board 12.20.22

The Safety Analysis Report (SAR) states that an explosion can occur when "hydrogen isotopes mix with oxygen, reach a flammable concentration, and an ignition source is present". Oxygen is introduced by in-leakage of the secondary confinement. Hydrogen is only introduced into the secondary confinement by a breach in the primary confinement. Both oxygen and hydrogen concentrations in secondary confinement are monitored and controlled. In addition, the stripper oxygen monitors provide an aggregate measure of oxygen concentration for all the secondary confinement environments. Therefore, multiple credited and non-credited SSC's are present to prevent or preclude an environment conducive to explosion. These mitigating factors lead SRTE and, ultimately, NNSA to accept a 60 day surveillance frequency for the HANM oxygen monitors as adequate.

Finally, the DNFSB noted failures of the oxygen sensor are not "self-revealing", however, that does not mean they are non-detectable. As noted in the discussion on health monitoring, a review of LCO data from 3/1/2019 to 2/28/2022 indicates Operations and Shift Technical Engineering identified 67% of oxygen cell failures in the facility during routine trending of process instrumentation.

Delta F Replacement Strategy

Replacement of a Delta F oxygen monitor is a complex evolution requiring new electrical and piping feedthroughs in the glovebox as well as new cabling in the process rooms. Depending on the complexity of a specific location, design and construction can cost $1M or more and, construction can require an outage of 30 – 40 days. While construction is in progress, the facility is in LCO 3.4.1 C which requires local alternate monitoring and additional operator rounds every 3 hours. Because loss of alternate monitoring would result in TSR implications, redundant alternate oxygen monitors are used.

Scheduling of these replacement activities requires a high degree of coordination with other projects to ensure space is available in the facility and interferences are managed. Coordination with construction services is required to ensure qualified personnel with appropriate clearance in each craft are available to work in the facility. Coordination is required with operations to ensure the work can be performed safely without disruption to other critical evolutions in the facility and the number of LCO's being actively managed at any given time in the facility are controlled. Finally, SRTE management must prioritize these projects with the other project priorities to match the funding profile authorized by the customer. Figure 7 below describes the road map for replacing the Delta F monitors. This road map is reviewed with management at each O_2 monitoring system health report, and the schedule is integrated into the facility project schedule as well as the facility Plan of the Week.

Received by the Board 12.20.22

Received by the Board 12.20.22

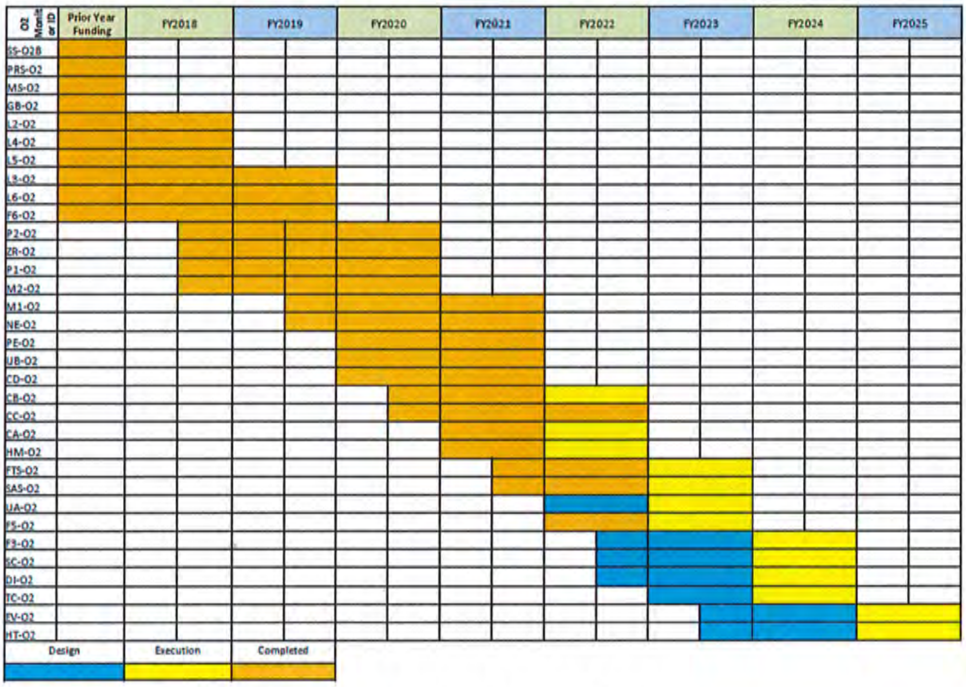

Figure 7: O_2 Monitor Upgrade Road Map

SRTE Engineering has maintained a schedule for replacing the Glovebox O_2 monitors since approximately 2010. This schedule reflects the realities of the existing funding profile, the facility production schedule, and the complex nature of managing safe operations in a nuclear facility. In fact, it was accelerated by over three years after it was demonstrated that the work could be performed within the operational and time constraints of LCO 3.4.1 condition C and Operations could safely and effectively manage the outage with minimal impact. Because of these successes, additional funding was allocated to increase the number of replacements per year. SRTE continues to look for opportunities to improve that schedule while managing the many other strategic improvements planned to improve safety and reliability in other critical areas of operations. To date, 70% of the Delta F O_2 monitors have been replaced in the field, with the remainder scheduled to be replaced by the end of FY25.

Management Expectations for Design Authority Engineers

Management focus on reliability as well as availability is a primary driver for all Design Authority engineers to be aware of events and issues related to their systems as reported in the STE shift logs and Operation's Status Boards. It is also a driver for management expectations that DAE's will walk down their systems at least weekly. These activities ensure the DAE is aware of, and takes action on, issues prior to a significant impact on operations. These expectations are actively managed and, do not require objective evidence of completion.

Received by the Board 12.20.22

Received by the Board 12.20.22

Conclusion

SRTE has a robust system monitoring program that complies with the SRS E7 manual. The program, as implemented, has effectively identified performance issues and maintains safety-related equipment at a high degree of availability. Performance issues, such as the Delta F O_2 Monitor failures, are being proactively resolved as evidenced by the replacement strategy presented and the improved performance of the Rosemount analyzers.

References

SRNS-T0000-2009-00007, Analysis of Tritium Facilities Glovebox Oxygen Monitors, P. J. Foster, et al., January 15, 2009.

WSRC-TS-96-17, Revision 32, Tritium Facilities Technical Safety Requirements (U), February 2022.

WSRC-SA-1-2-Vol-2, Revision 27, Tritium Facilities Safety Analysis Report, February 2022.

IEC/IEEE 60780-323, Nuclear Facilities – Electrical Equipment Important to Safety – Qualification – Edition 1.0, February 2016.

10CFR 830.122(c), Quality Assurance Criteria.

E7 Procedure 3.04, Revision 12, SSC Performance Monitoring, June 21, 2021.

Received by the Board 12.20.22