DEFENSE NUCLEAR FACILITIES SAFETY BOARD
Washington, DC 20004-2901

May 15, 2024

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

Dear Secretary Granholm:

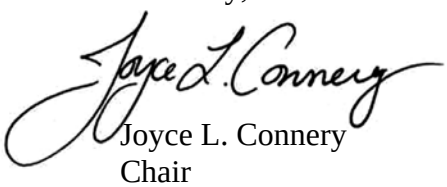
The Defense Nuclear Facilities Safety Board (Board) reviewed the final design of the continuous air monitor (CAM) system for the Waste Isolation Pilot Plant (WIPP) Safety Significant Confinement Ventilation System (SSCVS). The safety function of the CAM system is to detect a radiological release in the WIPP underground and to automatically align the SSCVS system into a safe configuration to avoid a radiological release to the surface.

The CAM system must perform its safety function in an environment with airborne combustion products from fire and salt particles from mining activities. However, the current WIPP management and operating contractor, Salado Isolation Mining Contractors, LLC, has not demonstrated that the CAM system will perform its safety function in this environment. In addition, for the subset of accident scenarios involving the waste shaft station in the hazard analysis, the SSCVS safety analysis credits initial conditions and administrative controls to reduce the risk but does not credit the engineered control offered by SSCVS. In the Department of Energy's published hierarchy, engineered controls are preferred over administrative controls due to the susceptibility to human errors inherent in administrative controls.

The enclosure further describes the Board's safety concerns. Pursuant to 42 U.S.C. §2286b(d), the Board requests a written response and briefing from DOE within 60 days of receipt of this letter, addressing the Board's safety concerns over whether the CAM system can reliably perform its safety functions in the expected operating environment. The Board notes

that the WIPP contractor recently changed its approach to starting up the CAM system. This new approach represents an opportunity to collect data to address some of the reliability concerns.

Sincerely,



Joyce L. Connery
Chair

Enclosure

c: Mr. William White, Senior Advisor, Office of Environmental Management
Mr. Mark Bollinger, Manager, Carlsbad Field Office
Mr. Joe Olencz, Director, Office of the Departmental Representative to the Board

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Report

Date: March 21, 2024

Final Design of the Continuous Air Monitor (CAM) System for the Safety Significant Confinement Ventilation System (SSCVS) at the Waste Isolation Pilot Plant (WIPP)

Summary. The Defense Nuclear Facilities Safety Board's (Board) staff team (staff team) reviewed the final CAM system design for SSCVS at WIPP. The safety function of SSCVS is to filter potentially contaminated underground air before it is released to the environment and to direct air to the waste face at the active waste panel to protect underground workers. The safety function of the CAM system is to detect a radiological release in the underground, transmit a signal to the central monitoring room, and automatically actuate isolation dampers to avoid a radiological release to the environment.

The isolation dampers are located between the salt reduction system and the SSCVS filtration system and are designed to divert the underground air flow from the salt reduction building to the new filter building in the event of an underground release. The salt reduction system is not safety significant and is not part of the SSCVS credited safety significant confinement boundary.

The SSCVS hazard analysis [1] identifies underground radiological accidents with high consequences to the collocated worker. Most of these accidents involve fire and may occur during mining activities. Mining activities produce a significant amount of salt particles that get suspended in the air. For that reason, the CAM system has the potential to operate in an environment with airborne combustion particles from fire and salt particles from mining activities. However, the current WIPP management and operating contractor, Salado Isolation Mining Contractors, LLC (SIMCO), has not demonstrated that the CAM system will operate reliably in the environment of airborne salt particles from normal mining operations, which could be exacerbated with fire particles in the case of a fire scenario.

Further, DOE Standard 3009-2014 prioritizes engineered controls over administrative controls [2]. However, the hazard analysis for the project uses administrative controls and not the SSCVS to reduce the risk of accidents at the waste shaft station. The accident scenarios identified in the hazard analysis occur in three main areas of the underground: (1) the waste shaft station, (2) the transport path, and (3) the active waste panel. To reduce the risk of accidents at the transport path and active panel, SIMCO credits preventive administrative controls and SSCVS as an engineered mitigative control [3]. However, SIMCO only credits administrative controls to reduce the risk of accidents at the waste shaft station. Due to the inherent likelihood of human error of administrative controls, the SSCVS should be used as an engineered control to reduce the risk of accidents at the waste shaft station.

The staff team also observed a lack of Department of Energy (DOE) Carlsbad Field Office (CBFO) oversight in the areas of electrical and instrumented safety systems due to

staffing shortages. Lastly, the staff team confirmed that SIMCO addressed a safety issue identified in the Board's 2019 letter on SSCVS [4] by incorporating an interlock between the SSCVS fans and the utility shaft fans to reduce the risk of an underground air flow imbalance and inadvertent release of unfiltered potentially contaminated air.

Background. In the current WIPP safety basis, waste emplacement activities are prohibited when operating the ventilation system in unfiltered mode during periods of mining activity [5]. On the other hand, the SSCVS preliminary documented safety analysis (PDSA) [3] allows waste emplacement and mining activities to occur simultaneously. The SSCVS safety design strategy [6] requires the CAMs to be qualified to operate in the environment of concern, namely an environment containing (1) airborne salt, (2) fire combustion particles and, (3) the combination of airborne salt and fire combustion particles.

The Board previously expressed safety concerns with the safety design basis documents for the SSCVS project in a letter dated August 27, 2019. These safety concerns included: (1) the need for a complete final design of the CAM system, (2) inadequate isolation damper closure time, and (3) the lack of an interlock between SSCVS and the utility shaft fans.

On June 26, 2023, the staff team submitted an agenda to CBFO with lines of inquiry related to the CAM system final design for the SSCVS project, including detection, signal transmission, and actuation of automatic control upon underground radiological release. On August 15, 2023, the staff team discussed the agenda with SIMCO and CBFO personnel. This report documents the staff team's evaluation of the CAM system final design.

Discussion. The staff team reviewed the final design of the CAM system for SSCVS, including the hazard analysis, PDSA, and procurement documentation with a focus on the capability of the CAM system to perform its safety function. The review also evaluated the ability of the credited controls to reduce the risk of postulated underground events, CBFO oversight of the SSCVS project, and the approach to incorporate an interlock between the SSCVS fans and utility shaft fans. The staff team identified the following safety concerns.

CAM Design Does Not Meet Safety Integrity Level (SIL)-2 Requirements—Attachment 3 of DOE Order 420.1C, *Facility Safety* [7], requires:

> *Safety significant SSCs* [structures, systems, and components] *must be designed to reliably perform all their safety functions. This can be achieved through a number of means, including use of redundant systems/components, increased testing frequency, high reliability components, and diagnostic coverage (e.g., on-line testing; monitoring of component and system performance; and monitoring of various failure modes). DOE-STD-1195-2011*, Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities, *provides an acceptable method for achieving high reliability of safety significant safety instrumented systems.*

The focus of DOE Standard 1195 [8] is how to utilize the process industry standard, American National Standards Institute/International Society of Automation (ANSI/ISA)

84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* [9], to support the design of reliable safety significant instrumented systems. Specifically, Appendices A, C, and D provide additional information on the use of ANSI/ISA 84.00.01-2004.

The CAMs are part of a safety significant instrumented system consisting of airborne radiation detection sensors, logic solvers, and final actuation devices (the dampers that close to isolate the salt reduction system and direct mine exhaust to high efficiency particulate air filters).

DOE Standard 1195 provides performance requirements which drive the design of safety instrumented systems, as opposed to specifying prescriptive design requirements. These performance requirements are met by requiring the system design meet a specific SIL. The PDSA for SSCVS indicates that "*system performance and reliability are assured by meeting a SIL-2 or equivalent reliability in accordance with DOE-STD-1195-2011 requirements.*" SIL-2 reliability corresponds to a probability of less than 10^{-2} that the system will not perform its safety function when required, which equates to a risk reduction factor of at least 100.

DOE Standard 1195 and ANSI/ISA-84.00.01-2004 require verifying this reliability performance by a calculation. This reliability calculation considers component failure rates, component failure modes, effects of failure, surveillance test frequency, surveillance test efficiency, and system repair strategy, which may be delineated in the technical safety requirements.

The national consensus standard upon which the DOE standard is based, ANSI/ISA-84.00.01-2004, requires that components used in safety instrumented systems be suitable for use. Evidence of suitability includes the following:

- Consideration of the manufacturer's quality, management, and configuration management systems;
- Adequate identification and specification of the components or subsystems;
- **Demonstration** of the performance of the components or subsystems **in similar operating profiles and physical environments** [emphasis added]; and
- The volume of the operating experience.

The estimated failure rate of the components in any mode that would cause a dangerous failure of SSCVS and remain undetected by the diagnostic tests is one of the inputs to the SIL verification calculation. For CAMs, a dangerous failure is a failure that would result in a CAM failing to detect and respond to a radioactive release event. The SIL verification calculations used a value of 4.2289×10^{-6} failures per hour for the dangerous undetected failure rate of the CAM in the SSCVS design (Mirion iCAM-HD™). The source of the CAM failure rate is a report from Mirion Technologies [10]. ANSI/ISA-84.00.01-2004 also notes:

> [T]*he estimated rates of failure of a subsystem can be determined by a quantified failure-mode analysis of the design using component or subsystem failure data from a recognized industry source or from experience of the previous use of the*

subsystem ***in the same environment as for the intended application*** [emphasis added], *and in which the experience is sufficient to demonstrate the claimed mean time to failure on a statistical basis to a single-sided lower confidence limit of at least 70%.*

CAMs in the WIPP mine are subject to inflow of airborne salt particles. The CAMs are also required to perform their safety functions while being subject to a smoke-filled environment resulting from a postulated accident event that the safety instrumented system is designed to mitigate. Despite sufficient air flow, airborne particles of salt and combustion products may build up on the detector, shielding alpha and beta radiation from reaching the detector (Figure 1). This could affect the detector's performance before the accumulated particulate obstructs the airflow through the CAM sufficiently to trigger a protective action from the safety instrumented system to align SSCVS into a safe configuration to avoid a radiological release to the surface. This would impact the ability of SSCVS to perform its safety function. The magnitude of this shielding effect has not been evaluated or quantified. Even though the design uses a CAM array consisting of three separate CAMs, any of which can initiate the safety function, they are all subject to the same environment, which can serve as a potential common mode failure initiator.

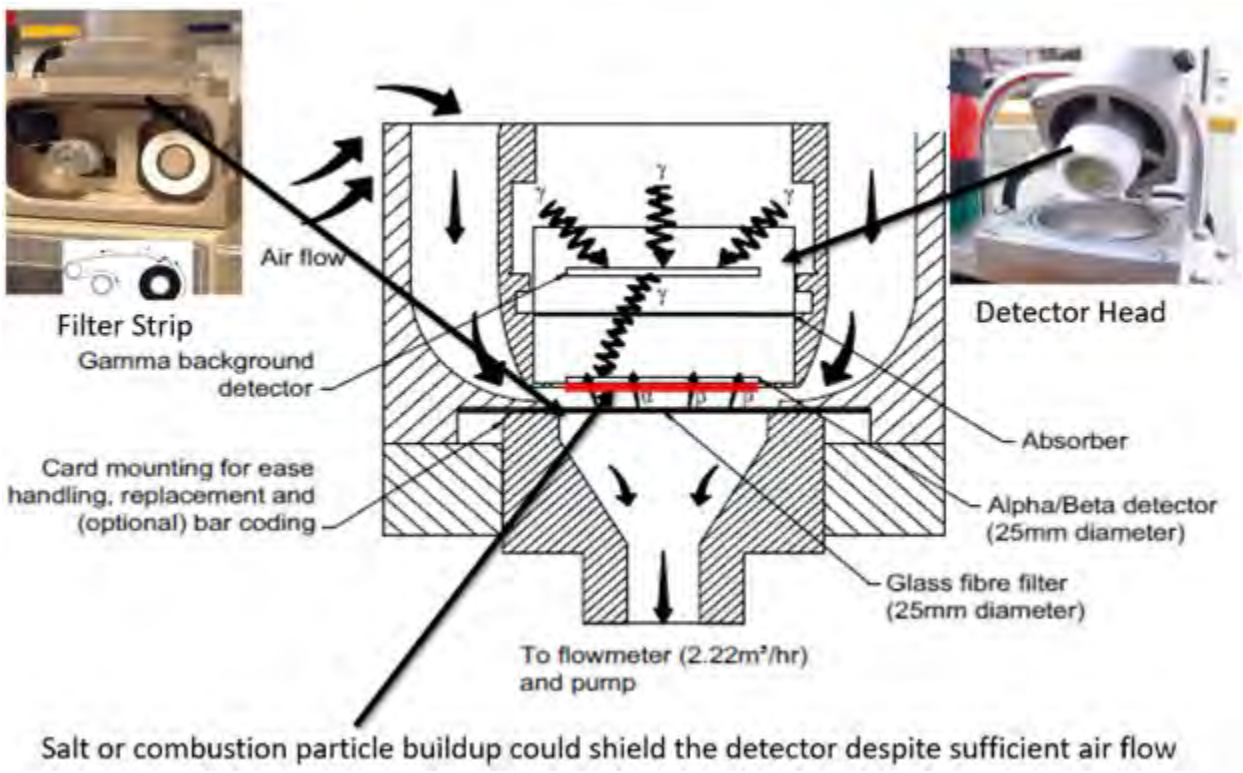


Figure 1. *Representative CAM Design (adapted from* [11]*)*

SIMCO has maintained that the operating environment is not considered as part of the SIL analysis. This amounts to an assertion that the operating environment has no effect on component reliability. However, the environment in which the safety significant CAMs operate

could have a significant impact on their performance, as recognized in ANSI/ISA-84.00.01-2004.

The CAMs are the most robust version available from the manufacturer and have been fitted with titanium-clad detectors to better withstand the salt dust environment. But this does not mitigate the potential alpha and beta particulate shielding effects from particle buildup. The effects of the environment in which the CAMs operate should be further evaluated to ensure it will not affect performance of the CAMs' safety function. Ideally, this evaluation should be supported by test data.

SSCVS is not used as a Safety Control to Mitigate Accidents at the Underground Waste Station—Transuranic waste is present at three main areas in the underground: (1) the waste shaft station during waste download; (2) the transport path while waste is being moved from the waste shaft station to the waste panel; and (3) the active waste (disposal) panel where the waste is permanently emplaced (Figure 2). Accident events with high consequences to the collocated worker have been identified in these three areas [1]. CAMs are located at the disposal panel. Additional CAMs could be located at the waste shaft station.

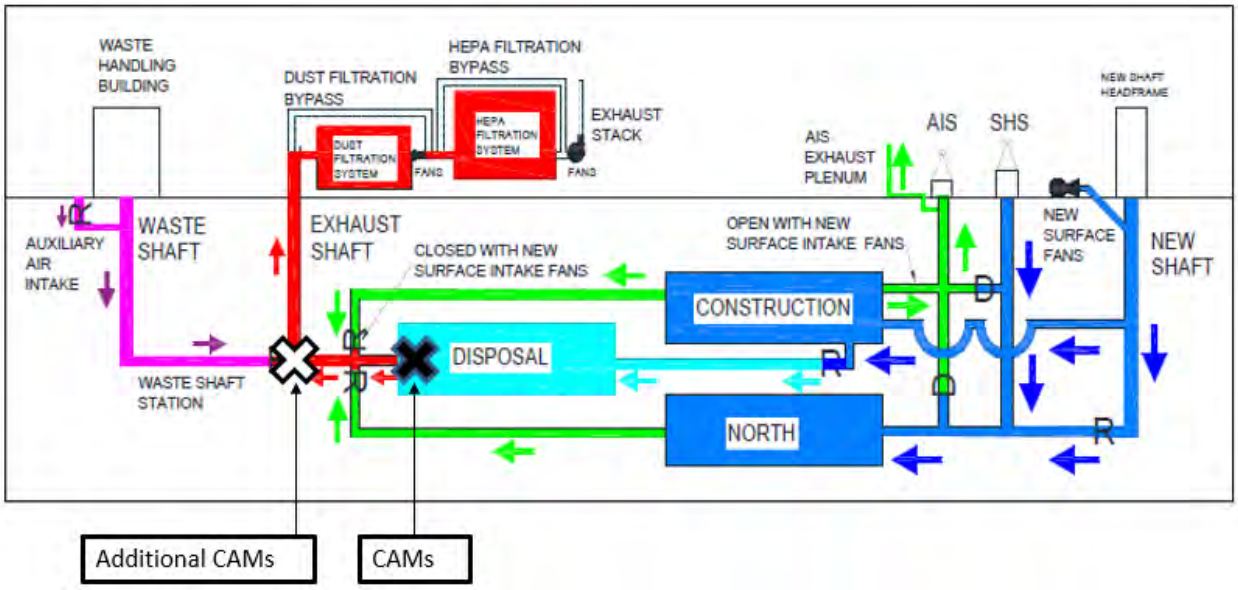


Figure 2. *Illustration of Underground Airflow*

SIMCO will credit the initial condition [12], the administrative controls, and the engineered control to reduce the risk of postulated events along the transport path and at the waste panel. However, SIMCO only credits the initial condition and administrative controls for the waste shaft station (Table 1). DOE Standard 3009-2014 [2] establishes that due to the inherent uncertainty of human performance, engineered controls are preferred over administrative controls.

Table 1. *Credited Controls for Postulated Events in Underground Locations*

		Waste Shaft Station	Transportation Path	Active Waste Panel Exhaust
Administrative Preventive Controls	Vehicles/equipment pre-operational checks and Spotters	Yes	Yes	Yes
Engineered Mitigative Controls	SSCVS/CAMs	No	Yes	Yes

Crediting SSCVS/CAMs as an engineered control for accidents at the waste shaft station would require locating CAMs at the waste shaft station near bulkhead 308. It would also require a damper actuator capable of isolating the salt reduction system in 30 seconds or less [4] [13]. SIMCO confirmed that the damper's actuator will be capable of isolating the salt reduction system in as little as five seconds [14].

Based on DOE's preferred hierarchy of controls and the capability of the CAM system to perform this safety function at the waste shaft station, the omission of SSCVS/CAMs as a credited control for these potential accidents is inconsistent with DOE Standard 3009-2014.

Lack of CBFO Oversight in Instrumentation and Controls—The staff team noted that there was a lack of federal oversight, specifically with regard to electrical and instrumented safety systems. CBFO personnel acknowledged this issue and have brought in direct support contractors to perform federal oversight in this area. CBFO personnel also mentioned that they are in the process of hiring for the federal electrical safety system oversight position. The lack of oversight is another data point on the larger CBFO federal oversight problems identified in recent Board correspondence (see, for example, the Board Letter regarding DOE Oversight Effectiveness dated August 17, 2022 [15]).

Functional Classification of the Interlock Between the SSCVS Fans and Utility Shaft (5th Shaft) Fans—In 2019, the Board identified [4] the need for an interlock between the SSCVS fans and utility shaft (5th shaft) fans. After further evaluation [16], WIPP personnel acknowledged that if the SSCVS fans stop operating while the utility shaft fans continue to operate, the resulting imbalance of the underground airflow could lead to an inadvertent release of unfiltered air from the disposal air circuit. In 2020, DOE informed the Board that the SSCVS project had committed to install such an interlock, but that its functional classification required further analysis of the reconfigured mine airflow. SIMCO qualitatively determined [1] that the consequences to the public and workers would be low for the scenario where the filtered exhaust system shut down while the utility shaft ventilation continued to supply air into the underground potentially releasing contamination out of the other shafts to the surface. Therefore, an interlock to shut down the utility shaft ventilation on an indication of loss of exhaust flow is not required to be safety significant.

Conclusion. SIMCO has not demonstrated that the CAM system can perform its safety function in an environment with airborne salt and smoke particles. This could delay or deter the

automatic actuation of the damper to isolate the salt reduction system and prevent an unfiltered radiological release to the environment in the event of an underground radiological release. In addition, the controls to reduce the risk of a radiological release at the waste shaft station are not optimal. Using only administrative controls instead of a combination of administrative and engineered controls presents an unnecessary risk, especially since SSCVS is credited to mitigate accidents at the transportation path, and waste panel and isolation dampers can actuate quickly enough to mitigate accidents at the waste shaft station.

References

[1] Nuclear Waste Partnership LLC, *Hazards Analysis for the Waste Isolation Pilot Plant Transuranic Safety-Significant Confinement Ventilation System Safety Basis,* WIPP-021SSCVS, Rev. 0, January 2021.

[2] Department of Energy, *Preparation of Nonreactor Nuclear Facility Documented Safety Analysis,* DOE-STD-3009-2014, November 2014.

[3] Nuclear Waste Partnership LLC, *Waste Isolation Pilot Plant, Safety Significant Confinement Ventilation System Project, Preliminary Documented Safety Analysis,* 500655-416-BD-SE-00306, REV. 2, January 2023.

[4] Defense Nuclear Facilities Safety Board, *Letter from Chair Bruce Hamilton to DOE Secretary James Richard Perry, Safety Issues Relating to the Waste Isolation Pilot Plant Safety Significant Confinement Ventilation System,* August 27, 2019.

[5] Nuclear Waste Partnership LLC, *Waste Isolation Pilot Plant Documented Safety Analysis,* DOE/WIPP 07-3372, Rev.8, September 2022.

[6] Nuclear Waste Partnership LLC, *Safety Design Strategy of Waste Isolation Pilot Plant Safety Significant Confinement Ventilation System, Revision 4.0F,* 500655-416-SE-DB-00300-F, March 2018.

[7] Department of Energy, *Facility Safety,* DOE Order 420.1C Chg 1 (PgChg), February 2015.

[8] Department of Energy, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities,* DOE-STD-1195-2011, May 2011.

[9] American National Standards Institute, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector-Part 1: Framework, Definitions, System, Hardware and Software Requirements, September 2004,* ANSI/ISA 84.00.01-2004 Part 1 (IEC 61511 Mod), September 2004.

[10] Mirion Technologies, Inc., *Mean Time Between Failure MTBF Report ICAM HD,* 1000001914, Rev B, October 19, 2022.

[11] Mirion Technologies, Inc., Terry Schwager, *Overview of Basic iCAM Operation,* July 2021.

[12] Department of Energy, Carlsbad Field Office, *Transuranic Waste Acceptance Criteria for the Waste Isolation Pilot Plant, Revision 9,* DOE/WIPP-02-3122, October 2018.

[13] SRK Consulting, *Ventilation Analyses in Response to DOE PPR of the SSCVS,* DN-486300.050-17, August 2020.

[14] The Industrial Company, *Curtiss Wright – Calculations for 10D 156”x156” Bubble Tight Dampers,* ARVR-515964-PQ-931-01, June 2023.

[15] Defense Nuclear Facilities Safety Board, *Letter from Chair Joyce L. Connery to DOE Secretary Jennifer M. Granholm, Review of DOE Safety Oversight Effectiveness,* August 17, 2022.

[16] SRK Consulting, *Ventilation Analyses in Response to DOE PPR of the SSCVS,* DN-486300.050-16, March 2020.