DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

June 2, 2008

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: J. L. Shackelford

SUBJECT: Review of the Design, Functionality, and Maintenance of Safety Systems at the Y-12 National Security Complex

This report documents a review of the design, functionality, and maintenance of safety systems at the Y-12 National Security Complex (Y-12). This review was conducted by members of the staff of the Defense Nuclear Facilities Safety Board (Board), T. Davis, D. Gutowski, D. Kupferer, D. Owen, C. Roscetti, and J. Shackelford during April 15–17, 2008.

Background. The staff conducted a review at Y-12 to assess the design, functionality, and maintenance of selected safety systems in Buildings 9212 and 9204-2E. The review focused on the design, safety basis, and other calculations and analyses for the selected systems, as well as the functional requirements for the systems during abnormal and accident conditions. The staff reviewed system test, surveillance, and maintenance activities to investigate how the acceptance criteria specified by these activities were adequately supported by design calculations or other engineering documents. The review included an assessment of the normal and emergency operations of the systems to determine whether those operations were governed by approved operating procedures and were consistent with the design basis.

The staff found that in general, the systems reviewed had adequately defined safety functions that were supported by appropriate system design calculations, instrument calibrations, system surveillances, and maintenance activities. Notwithstanding this conclusion, the staff developed several observations related to the conservatism of some of the design calculations and questioned whether some of the surveillance criteria fully bounded the system safety functions. The staff also noted weaknesses in the preventive maintenance procedures for some systems, and identified a number of activities that appeared to warrant additional pedigree, including designation as a safety control or improvements in existing administrative controls.

The following sections summarize the staff's observations on the safety systems that were reviewed at Y-12.

Building 9212 Holden Gas Furnace Interlocks. The Holden gas furnace uses natural gas to burn or dry small batches of uranium-bearing materials prior to further processing. The furnace is equipped with interlocks that are credited as a safety-significant system. Their function is to reduce the frequency of natural gas explosions by monitoring and shutting off the natural gas supply in response to a number of postulated abnormal conditions. The furnace and its attendant controls are designed and maintained in accordance with National Fire Protection Association (NFPA) 86, *Standard for Ovens and Furnaces*.

The staff noted that the safety function of the interlocks had been appropriately specified in the facility Documented Safety Analysis (DSA) and that adequate Technical Safety Requirement (TSR) surveillance tests had been developed to periodically verify that the system would perform its intended safety function. The system set points had been adequately determined and documented in facility design analyses and calculation documents. Further, both the normal and abnormal operations of the system were governed by approved operating procedures.

However, the staff noted that the leak testing of the isolation block valves was performed at the system's normal operating pressure rather than at its maximum possible gas pressure. As a result, the current leak test does not necessarily ensure that the block valves would achieve adequate isolation during a credible overpressure situation.

On February 27, 2008, three of the five safety-related instruments associated with the interlocks were found to be out of the tolerance specified in the approved instrument calibration documents. The facility implemented corrective actions, which included readjusting two of the instruments and replacing the third. However, the staff noted not all requirements related to the analysis and documentation of out of tolerance conditions were met. In particular, it was not clear whether this incident had implications for the operability or for surveillance frequency of the interlocks during the out-of-tolerance condition. In response to the staff's concerns, the facility performed further investigations and developed a nonconformance report on the lack of documentation of the root cause and corrective actions associated with the out-of-tolerance incident.

Building 9212 Safety-Class Fire Protection Sprinkler System, and Building 9204-2E Safety-Significant Fire Suppression System. The sprinkler systems for Building 9212 (system 6) and Building 9204-2E (system 4) are classified as safety-class and safety-significant, respectively. These systems are credited with reducing the frequency of a small fire becoming a larger fire by providing fixed fire suppression with automatic initiation for certain areas in their coverage zones. The systems are designed, installed, and maintained in accordance with NFPA 13, *Standard for the Installation of Sprinkler Systems*.

The system in Building 9212 is equipped with low-temperature detection and alarm capability because certain sections of the building are located in areas with the potential for freezing temperatures. While there were no reported incidents of freezing associated with the system, a recent freezing incident involving the fire protection system in another facility had

temporarily rendered that system inoperable. The staff observed that the low-temperature detection and alarm system and heater, while an important support system for the safety-class fire protection system, lacked an appropriate safety pedigree. The staff believes that the support capabilities of the low-temperature detection and alarm system and/or heater warrant additional attention and consideration for an upgrade to safety-significant or improvements in the existing administrative controls related to cold weather operations.

The following additional observations apply to both the Building 9212 safety-class and Building 9204-2E safety-significant fire suppression systems.

The staff observed that system operability was based in part on a periodic pressure drop test and control of the system valve lineup. The pressure drop test consisted of verifying adequate system pressure at the facility inlet gauge, and then observing the pressure drop over a timed interval following the establishment of flow from the systems' main drain valve. Although this test appeared to satisfy NFPA requirements for the systems, the staff noted that Y-12 lacked any formal hydraulic flow calculations demonstrating that the systems could deliver the desired flow rates for the postulated design basis fires. This observation was discussed during previous reviews by the staff, as well as in correspondence from the Board, dated October 16, 2003.

The controlled valve lineup used to ensure system operability did not include verification of the position of the isolation valves for the systems' pressure gauges. Without such a check, these valves could be mispositioned and isolate the pressure gauges, resulting in an indicated pressure higher than that which actually exists in the system. Further, the 5-year preventive maintenance procedure for the systems was written from a generic perspective, rather than being tailored to identify specific system components by their unique identifiers. As a result, maintenance personnel could inadvertently omit important system components from the required maintenance activities. The staff also observed that the equipment list containing the systems' sprinkler heads identified the equipment by location (batch tracking) instead of individually. Such an approach may not consistently provide a sufficient level of configuration management for safety-related systems.

The emergency response strategy for a facility fire involved connecting a fire pumper truck to connections on the exterior of the affected facilities. This activity was designed as a precautionary measure to ensure that adequate system pressure is available during an emergency in the event of a loss or degradation of normal system pressure. However, Y-12 personnel noted that the pumper truck was capable of developing pressures in excess of the maximum allowable pressures for the Building 9212 and 9204-2E systems. Thus, the systems could be overpressurized (and potentially damaged) during a fire emergency. Although the pressure developed by the pumper truck is controlled by the operator (by means of settings on an on-board regulator), the staff saw no evidence of controls or explicit precautions to ensure that the facility fire suppression systems would not be overpressurized.

Building 9212 Accountable Steam Condensate Automatic Isolation. The accountable steam condensate isolation unit is categorized as a safety-significant feature credited with protecting against a criticality accident in geometrically unfavorable equipment (i.e., the storm sewer). The system is composed of a conductivity monitor and isolation valve whose functions are to monitor and detect elevated conductivity in the accountable steam condensate and to shut the isolation valve within specified time limits to prevent the sudden release of a critical mass of uranyl nitrate into the facility storm sewer.

The staff observed that the system's safety function had been adequately described in the facility safety analyses and was supported by system design and set point calculations. However, the staff noted that the maximum credible concentrations of the operating process streams were not used in calculating the system set point. Rather, the values chosen reflected the high end of the normal operating range. These values are important in determining the allowable closure time for the isolation valve. Higher postulated concentrations would result in lower allowable valve closure times. The system engineer acknowledged that the maximum values had not been used, but stated his belief that the use of higher values would not change the valve closure time requirement because of other conservatisms present in the analysis. On the basis of available information, however, the staff was unable to independently verify whether the allowable closure time would be affected.

The surveillance test used to determine system operability warrants improvement in that it merely implies, rather than directly verifies, that the system will isolate at the credited set point for high conductivity. The conductivity monitor used to initiate the valve isolation is calibrated using one-point calibration at the system set point. However, based on discussions with Y-12 personnel it was learned that the functional test used to verify that the isolation valve will respond to the high-conductivity signal generated by the monitor is performed (using a standard solution) at 2000 micro-siemens per centimeter (uS/cm), rather than at the credited set point of 1000 uS/cm. As a result, the surveillance does not provide an integrated test of the safety function, as would be demonstrated by verifying that the isolation valve shuts at the credited set point.

Building 9212 Hydrogen Fluoride/Nitrogen (HF/N_2) Differential Pressure Interlock. The HF/N_2 differential pressure interlock is a safety-significant system credited with isolating the HF supply during postulated system upset conditions to reduce the consequences of HF backflows into the N_2 system. The safety function of the interlock was appropriately specified in the facility DSA, and adequate TSR surveillance tests have been developed to periodically verify that the system would perform its intended safety function. The system set points have been appropriately determined and documented in facility design analyses and calculation documents. Further, both the normal and abnormal operation of the system was governed by approved operating procedures.