Sean Sullivan, Chairman
Bruce Hamilton, Vice Chairman
Jessie H. Roberson
Daniel J. Santos
Joyce L. Connery

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Washington, DC 20004-2901

August 7, 2017

Mr. James Owendoff
Acting Assistant Secretary for Environmental Management
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Mr. Owendoff:

The alternative methodology approved by the Department of Energy (DOE) Office of River Protection for determining the safety integrity level of instrumented systems at the Low-Activity Waste Pretreatment System (LAWPS) does not provide an equivalent level of safety as required by DOE Order 420.1C, *Facility Safety*.

Specifically, the use of the alternative methodology may result in safety instrumented system designs that do not meet DOE's intent for reliable performance as well as safety strategies that do not incorporate adequate defense-in-depth.

Although this poses no safety consequences for LAWPS, a similar application of the alternate methodology to other facilities may yield unacceptable consequences. For that reason, the enclosed report by our staff is provided for your information and use.

Sincerely,

Sean Sullivan
Chairman

Enclosure

c: Mr. Joe Olencz

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

June 12, 2017

MEMORANDUM FOR: S. A. Stokes, Technical Director

COPIES: Board Members

FROM: K. Deutsch, F. Bamdad, and P. Fox

SUBJECT: Alternative Methodology for Safety Integrity Level Determination of Instrumented Systems at the Low-Activity Waste Pretreatment System

Members of the Defense Nuclear Facilities Safety Board's (Board) staff reviewed an alternative methodology, approved by the Department of Energy's (DOE) Office of River Protection (ORP), for determining the required safety integrity level (SIL) of instrumented systems at the Low-Activity Waste Pretreatment System (LAWPS). LAWPS personnel used this methodology in lieu of the methodology specified in DOE Standard 1195-2011, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities*.

DOE Order 420.1C, *Facility Safety*, states that alternative methods used in place of DOE technical standards that are determined to be applicable to the facility design or operation must demonstrate a level of safety equivalent to the replaced standard. The Board's staff assessed whether DOE Standard 1195 is applicable to the design of LAWPS and if the alternative method provides the equivalent level of safety required by the DOE order. On November 1, 2016, and March 16, 2017, the Board's staff team held teleconferences with ORP and Washington River Protection Solutions (WRPS). The objective of the discussions was to clarify the technical bases for requesting and granting the relief, and to determine how the use of the alternate SIL determination methodology could affect the design of the LAWPS Safety Instrumented Systems (SIS).

Background. DOE Order 420.1C requires safety significant structures, systems, and components (SSC) to be designed to reliably perform all their safety functions. The order states that 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). The order also requires that the facility design include multiple layers of protection (as part of the design defense-in-depth) to prevent or mitigate the unintended release of radioactive materials to the environment. DOE Standard 3009-2014, *Preparation of Nonreactor Nuclear Facility Documented Safety Analysis*, supports this requirement by specifying the use of multiple independent layers of defense so that the design

does not completely rely upon any one layer by itself, no matter how effective it is expected to be.

DOE Standard 1195 provides requirements and guidance for the design, procurement, installation, testing, maintenance, operation, and quality assurance of SISs with safety significant functions at DOE nonreactor nuclear facilities. These facilities use SISs for various control functions such as safety interlocks and process alarms. DOE Standard 1195 applies requirements of an industry standard, ANSI/ISA 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* (ISA 84), to support the design of reliable safety significant SISs at defense nuclear facilities.

ISA 84 and its predecessor, ANSI/ISA 84.01-1996, *Application of Safety Instrumented Systems for the Process Industries*, have been a source of requirements for the design of SISs at DOE nonreactor nuclear facilities for more than 20 years. A key input parameter for the use of these standards is the required SIL. The SIL is a discrete value that broadly specifies the reliability performance of the safety system. The lowest SIL value is one, while the highest SIL value is four. Each higher SIL value is a factor of 10 improvement in reliability. SIL-1 defines a probability of failure on demand range of 10^{-1} to 10^{-2} or a risk reduction factor of 10 to 100. ISA 84 and its predecessor leave the determination of SIL requirements to the user of the standard.

Prior to the issuance of DOE Standard 1195, a standard method for determining the SIL requirements for SISs used in DOE nonreactor nuclear facilities did not exist. The SIL determination methodology established as the accepted method in DOE Standard 1195 is a deterministic method based on the number of independent protection layers (IPL) credited by the hazard analysis. Figure 1, an extraction of Figure B.2-1 in DOE Standard 1195, summarizes this methodology.

Approval to Use Alternate Methodology. On October 29, 2015, the LAWPS contractor, WRPS, requested ORP to grant a relief from implementation of DOE Standard 1195 and approve the use of an alternate program to implement ISA 84 for safety significant SISs [1]. The relief request stated that the proposed alternate program follows the same methodology as that prescribed in DOE Standard 1195 except for the method for determining the SIL requirements of the SIS. WRPS had developed and applied this alternate approach in its role as the operations contractor for the Hanford tank farms before DOE initially issued Standard 1195.

Figure 2 summarizes the SIL determination methodology of the WRPS-developed program. This figure is an extraction from Appendix J of the WRPS program document, TFC-ENG-DESIGN-C-47, *Process Hazard Analysis*. The relief request also discusses that for a particular SIL value, the WRPS methodology yields a more conservative result because the WRPS program requires the risk reduction factor of the SIS design to be at least at the mid-point of the range.

Number of IPLs		
	3	SIL-1
	2	SIL-2 (1)(2)
	1	SIL-2 (1)(2)

Figure B.2-1: SIL Determination Methodology

Note 1: Where an event may result in a prompt public fatality (due to chemical releases) or multiple prompt collocated worker fatalities, the design authority should consider increasing the SIL number of the SIS by one or credit an additional IPL.

Note 2: When an event (non-criticality) is not expected to result in a facility worker or collocated worker fatality, the design authority may consider decreasing the SIL number of the SIS by one.

Figure 1. *SIL determination table from DOE Standard 1195*

ORP concluded that the WRPS implementation of ANSI/ISA 84.00.01-2004 for LAWPS provides adequate assurance that safety significant SISs reliably perform their intended functions. On February 17, 2016, ORP approved the WRPS relief request [2].

Discussion. The WRPS methodology's use of hazard frequency as the principal factor in determining SIL requirements is a key difference from the DOE Standard 1195 approach, which is based on the number of IPLs that exist to mitigate the hazard. Safety SSCs in the LAWPS design that are subject to this discussion are:

- Standby tank exhaust system (STES) to mitigate flammable gas accumulation in tank headspaces;
- Gas removal system (GRS) to mitigate flammable gas accumulated in the ion exchange column resin;
- Misroute protection system (MPS) to prevent direct radiation hazards due to waste misroutes; and
- Process inventory monitoring system to protect flammable gas generation assumptions.

Table J-1. SIL (or SIL Equivalent) Determination for SIS (or SIA)[1].			
Consequence[2]	**Frequency**[3]		
	Anticipated	**Unlikely**	**Extremely Unlikely**
Public (P) [offsite]	SIL-2[a]	SIL-2[a]	SIL-1
Co-Located Worker (CL) [onsite]	SIL-2[a]	SIL-1	SIL-1
Facility Worker (FW)	SIL-1[b]	SIL-1	SIL-1

Notes:

[1] SIL-1 = SIL equivalent 1 and SIL-2 = SIL equivalent 2 when using this table (and notes) to determine the SIL equivalent for SIA [safety instrumented alarm].

[2] Consequences are as described elsewhere in this procedure.

[3] Frequency is as described elsewhere in this procedure.

[a] May be reduced to SIL-1 if an independent SS SSC, SAC [specific administrative control], AC [administrative control] Key Element is also selected.

[b] Shall be increased to SIL-2 if there are no other additional measures to protect the facility worker.

Figure 2. *SIL determination table from WRPS methodology*

WRPS stated to the Board's staff that, under its interpretation of DOE Standard 1195, application of the standard would require the designs of all four SISs to meet SIL-2 requirements, including achieving a minimum risk reduction factor of 100. However, under the WRPS implementation of ISA 84, these designs will only be required to meet SIL-1 requirements based on frequency and consequence evaluations. The WRPS program requires a SIL-1 design to meet a minimum risk reduction factor of 50.

ISA 84 places additional requirements on a SIL-2 design beyond meeting higher risk reduction factor values. The historical approach to safety system design is to ensure that no single fault would result in loss of intended function. ISA 84 and other modern functional safety standards have adopted the concept of SILs with increasing performance depending on the need for risk reduction in the specific application involved. ISA 84 adds fault tolerance requirements based on the required SIL to ensure the resulting design is robust against both random hardware and systematic faults. In general, this drives the design to consider some architectural requirements (i.e., redundancy) to meet requirements for higher SILs.

WRPS stated to the Board's staff that achieving SIL-2 for STES and GRS would present additional design challenges. To achieve the increased risk reduction factor associated with SIL-2 would require combinations of additional redundancy, diversity, and surveillance test frequency. Also, the active nature of these systems poses additional challenges to develop fail-safe designs.

DOE Standard 1195 considers DOE Order 420.1C and DOE Standard 3009 defense-in-depth requirements by requiring multiple IPLs and specifying the following characteristics of each IPL:

- The IPL shall be designed to prevent an event or to mitigate the consequences of an event to a level that is supported by the safety basis documents.

- The IPL safety function shall be identified and documented in the safety basis documents of a facility.

- The IPL shall be designed to perform its safety function during normal, abnormal, and design basis accident environmental conditions for which it is required to function.

- The IPL shall be sufficiently independent so that the failure on one IPL, or of a component or subsystem of an IPL, does not adversely affect the probability of failure of another IPL credited for the same event.

- An IPL shall be independent from the cause of the safety significant event. A process system (e.g., ventilation, cooling water) that is not functionally classified as safety significant or safety class should only be identified as an IPL if its functions are implemented for the purposes of risk reduction, and if its components and the basic process control system are independent from the initiating event.

During the teleconferences, the Board's staff team asked WRPS about the existence of credited defense-in-depth or IPLs that augmented the protections provided by the STES, GRS and MPS. WRPS responded that for the STES and GRS, the technical safety requirement for ignition controls is the key administrative control contributing to defense-in-depth. The documented safety analysis would credit the normal non-safety building/vault/vessel ventilation system for the STES, the non-safety elution system for the GRS, and the non-safety process control system for the MPS as defense-in-depth features. Table 1 summarizes these defense-in-depth features. At the time of the teleconferences, WRPS indicated that it did not anticipate that the LAWPS safety basis would credit additional IPLs or defense-in-depth features.

Table 1. *Credited protection layers identified by WRPS*

Hazard	SIS	Other Credited Protection Layers
Flammable gas accumulation in the tank headspaces	STES	Ignition Controls Non-safety ventilation system
Flammable gas accumulation in the ion exchange column	GRS	Ignition Controls Non-safety elution system
Waste misroutes	MPS	Non-safety process control system

Crediting the non-safety ventilation system as an IPL for the removal of flammable gas in the tank headspaces violates the requirements for IPLs specified in DOE Standard 1195. Its loss can be the initiator of the safety significant event. Similarly, failures of the non-safety process control system can be the initiator of postulated misroute accidents. Consequently, the non-safety process control system cannot be credited as an IPL for these events. Further, DOE Standard 1195 states that administrative control programs, such as the proposed ignition controls, must be identified in the technical safety requirements in order to be credited as IPLs. WRPS has not indicated such an intent in its safety design strategy or in its SIS design. Because it is not appropriate to credit ignition controls, non-safety ventilation, or the non-safety process controls system as defense-in-depth, there is no credited defense-in-depth for both the flammable gas accumulation event in a tank headspace or the misroute event, and only one defined defense layer for preventing a flammable gas event in an ion exchanger column. DOE Standard 1195 would require at least two independent layers besides the SIS to permit the SIS to be designed to meet SIL-1 for each case.

Summary and Conclusions. DOE Order 420.1C refers to DOE Standard 1195 as an acceptable method for achieving high reliability of safety significant SISs. The order requires this standard to be considered applicable when it provides relevant design requirements for safety significant SISs. The order states that relief to DOE technical standards determined to be applicable to the facility design requires the use of methods that demonstrate an equivalent level of safety (i.e., meets or exceeds the level of protection) and are approved by the DOE field office.

The Board's staff team found that the WRPS SIL determination methodology yields a SIL-1 design requirement in cases where WRPS states that DOE Standard 1195 would require a SIL-2. DOE Standard 1195 allows a SIL-1 design if additional IPLs are identified and credited in the safety basis or where a failure of the SIS is not expected to result in a facility or collocated worker fatality (note 2 of Figure 1). However, WRPS has not identified additional IPLs in its strategy and indicated that note 2 of Figure 1 (the DOE Standard 1195 SIL determination table) does not apply to LAWPS.

Additionally, the use of the alternative method in other designs may yield a different SIL level design than specified DOE Standard 1195. Consequently, the alternate WRPS SIL determination methodology does not meet the equivalent level of safety requirement of DOE Order 420.1C and should not be considered an adequate replacement for DOE Standard 1195.

Lastly, the Board's staff team found that the existing design described by WRPS does not provide adequate defense-in-depth, as required by DOE Order 420.1C and DOE Standard 3009. DOE Standard 1195 implements this requirement through the application of IPLs that must meet specific characteristics. As discussed above, the defense-in-depth features for the STES, GRS, and MPS do not meet these characteristics.

References.

1. Letter, Mr. Mark Lindholm, President and Project Manager to Kevin W. Smith, Manager, *Contract Number DE-AC27-08RV14800 – Washington River Protection Solutions LLC Request for Relief from DOE-STD-1195, Design of Safety Significant Safety Instrumented Systems Used at DOE Non-Reactor Nuclear Facilities*, WRPS-1504409, October 29, 2015.
2. Letter, Kevin W. Smith, Manager to Mr. Mark Lindholm, President and Project Manager, *Contract Number DE-AC27-08RV14800 – Approval of Washington River Protection Solutions LLC Request to Continue to Use the Currently Implemented Industry Standard ANSI/ISA-84.00.01-2004 in lieu of DOE-STD-1195 for the Low-Activity Waste Pretreatment System Project*, 15-NSD-0033, February 17, 2016.