U.S. DEPARTMENT OF ENERGY

PNNL-19310

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Safeguard By Design Lessons Learned from DOE Experience Integrating Safety into Design

J Hockert
RL Burbank

April 2010

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)

PNNL-19310

Safeguard By Design Lessons Learned from DOE Experience Integrating Safety into Design

John W. Hockert
Contractor with XE Corporation
RL Burbank

April 2010

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Abstract

This paper identifies the lessons to be learned for the institutionalization of Safeguards by Design (SBD) from the Department of Energy (DOE) experience developing and implementing DOE-STD-1189-2008, *Integration of Safety into the Design Process*. The experience is valuable because of the similarity of the challenges of integrating safety and safeguards into the design process. The paper reviews the content and development of DOE-STD-1189-2008 from its initial concept in January 2006 to its issuance in March 2008. Lessons learned are identified in the areas of the development and structure of requirements for the SBD process; the target audience for SBD requirements and guidance, the need for a graded approach to SBD, and a possible strategy for development and implementation of SBD within DOE.

Contents

1.0 Introduction and Purpose

This paper presents the lessons to be learned for the institutionalization of SBD from the DOE experience with the institutionalization of DOE-STD-1189-2008. The lessons learned were developed by reviewing 1) the institutional drivers and impediments to the development of DOE-STD-1189-2008, 2) the approach taken by DOE in the development and institutionalization of SBD, and 3) the experience of DOE contractors in implementing DOE-STD-1189-2008. These reviews included data collection from published sources and from interviews with people directly involved with the development, institutionalization, and application of DOE-STD-1189.

The paper presents conclusions and recommendations for policy makers (DOE, Nuclear Regulatory Commission [NRC], or IAEA) responsible for managing the development and implementation of the SBD process based upon the DOE experience with DOE-STD-1189-2008. These conclusions and recommendations are intended to be applicable to a general SBD process. *However, because the scope of this study was limited to DOE activities, additional confirmatory studies of similar activities, such as IAEA efforts to integrate safety with design and project management, would be beneficial to provide additional assurance that the conclusions are not distorted by unique aspects of the DOE environment.* Additional detail about the bases for these recommendations and conclusions can be found in the report[1] that forms the basis of this paper.

As early as 2005, DOE senior management recognized the need to revise the DOE directives and guidance for project management for the acquisition of capital assets to provide "more complete description of safety expectations for early design steps." [2] The drivers for revision were analyses of the causes of cost and schedule overruns on large design and construction projects [3] and Defense Nuclear Facilities Safety Board (DNFSB) interest in the integration of safety into the design process. In December 2005, the DNFSB initiated a series of public meetings and hearings on the DOE and National Nuclear Security Administration (NNSA) incorporation of safety into the design and construction of defense nuclear facilities. In December 2005, the Deputy Secretary directed that actions to revise the project management directives and guidance to enhance integration of safety into design be initiated in January 2006 [2]. By July 2006, DOE planned to include the requirements for integration of safety into the design process for Hazard Category 1, 2, and 3 nuclear facilities into a new DOE-STD-1189-2008, Integration of Safety into the Design Process, which was scheduled to be issued in calendar year 2006 [4]. However, the development of the standard required more time than anticipated, and the draft of DOE-STD-1189-2008 was released for DOE-wide review on March 30, 2007 [5]. The DNFSB continued to monitor the development and institutionalization of DOE-STD-1189-2008, holding additional public meetings in March 2007. The review and approval of DOE-STD-1189-2008 also required more time than anticipated, with the final approved standard finally issued in March 2008 [6].

Reasons that the development, review, and approval of DOE-STD-1189-2008 required more time than anticipated are discussed below in the lessons learned. However, it is important to realize that the internal drivers (i.e., the perceived impact of safety integration deficiencies on project cost and schedule) and external drivers (DNFSB monitoring of DOE progress) for integration of safety into design were much stronger than the corresponding drivers for institutionalizing SBD appear to be. DOE senior management was so strongly committed to the development and institutionalization of DOE-STD-1189-2008 that the effort could not be

permitted to fail.[1] Since this level of support and commitment may not currently exist for institutionalizing SBD, it is important to avoid potential missteps like the ones that delayed the institutionalization of DOE-STD-1189-2008.

[1] For example the 2006 *Annual Report to Congress on DOE Activities Relating to the DNFSB* (Reference 7) states on page II-16, that "DOE STD-1189 will provide the key course of action for ensuring that safety is incorporated into the baseline design of the Department's nuclear facilities."

2.0 Lessons Learned

The lessons to be learned from the development and implementation of DOE-STD-1189-2008 are divided into two categories. The first relates to content and presentation of the integration approach mandated in DOE-STD-1189-2008. The second category relates to the DOE experience in implementing DOE-STD-1189-2008, including the institutional development and approach taken to securing Departmental review and approval of DOE-STD-1189-2008. Both of these aspects of the institutionalization of the requirements for the integration of safety into the design process provide potentially useful lessons for the institutionalization of SBD.

The review of the requirements for integration of safety into the design process and their presentation in DOE-STD-1189-2008 identified the following good practices:

- **Mandatory Early Establishment of Expectations and Review of Approach by Owner / Regulator.** One of the major changes instituted by DOE-STD-1189-2008 is the requirement for DOE to provide early direction in three important aspects of safety in design. DOE is required to document its expectations regarding the formality and rigor of activities to integrate safety into design before conceptual design begins. DOE reviews and approves a safety design strategy prepared by the project early in conceptual design. DOE reviews and approves a conceptual design safety report prepared at the end of conceptual design [6].
- **Mandatory Early Participation by Subject Matter Experts and Establishment of Integration Mechanism.** DOE-STD-1189-2008 requires the project team to establish, during the early part of conceptual design, an interdisciplinary team, referred to as the Safety Design Integration Team (SDIT), which includes nuclear safety subject matter experts, experts from other disciplines, and design leads. The SDIT is responsible for activities to ensure that safety is integrated into design, including overseeing the preparation of the project's nuclear safety deliverables, such as the safety design strategy and the conceptual safety design report [6].
- **Mandatory Early Planning and Graded Approach for Safety.** The requirements discussed above for early establishment of safety in design expectations by the owner / regulator, for development of a safety design strategy and its early approval by the regulator and for early participation by subject matter experts, ensure that safety requirements are included early in project planning. DOE-STD-1189-2008 also t permits projects to use the documented safety design strategy to tailor the application of the requirements for integration of safety into design based upon the complexity and hazard of the facility.[2] This approach helps ensure that the DOE-STD-1189-2008 approach can be applied cost effectively across the broad spectrum of DOE facilities [6].
- **Conservative Risk Management Approach.** DOE-STD-1189-2008 requires that the project risks associated with safety issues are identified early and incorporated into overall project risk management [6]. It also seeks to foster a risk management approach in

[2] The use of the safety design strategy document for tailoring is discussed in Sections 2.3 and 2.4.4 of DOE-STD-1189-2008.

which these risks are managed by taking a very conservative approach toward the design of safety measures early in design and, where the design evolution or safety research permits, the conservatism is relaxed as the design progresses [8]. This approach is intended to ensure that most of the surprises associated with implementation of safety measures later in the design are pleasant ones, resulting in cost and schedule savings. However, this is one area where the approach mandated by DOE-STD-1189-2008 has not been as effective as its authors intended [8]. Thus, it may be worthwhile to see whether approaches other than those analogous to the DOE-STD-1189 requirements in this area might be more effective for SBD.

- **Identification of Key Project Interfaces That Affect Safety Design Decisions.** DOE-STD-1189-2008 provides a discussion of the key project interfaces that affect decisions on safety strategies and measures in Chapter 7 [6]. Section 7.8 specifically addresses the interfaces and interactions with security, which is used in DOE-STD-1189-2008 in a manner that would include international safeguards, where required for a DOE facility. A similar discussion would be valuable for SBD guidance or requirements so that safeguards subject matter experts could be alerted to project decisions that could affect the selection and effectiveness of safeguards measures.
- **Identification of the End of Conceptual Design as the Key Point Where Basic Design Approaches and Parameters Need to Be Established.** As the preceding discussion shows, the DOE-STD-1189-2008 requirements establish the end of conceptual design as the point where the designers have identified and evaluated the hazards associated with the proposed facility, identified the major safety functions necessary to provide adequate protection, identified safety structures, systems, and components (SSC), on a preliminary basis, and identified the major standards that these SSC will need to meet [6]. This is extremely important because the decisions made during conceptual design commit as much as 80% of the total life-cycle costs [9]. Use of this approach in SBD would require the IAEA and State regulatory authorities to modify their regulatory approach to provide for earlier submittal and review of facility design information and safeguards measures because under the approach review of this information typically does not begin until near the end of final design (i.e., about the start of construction).

The review of the requirements for integration of safety into the design process and their presentation in DOE-STD-1189-2008 identified the following areas for improvement:

- **Presentation of Requirements.** Some of the statements in DOE-STD-1189-2008 that have been interpreted by DOE and others as requirements are not clearly identified as requirements. For example, Preliminary Criticality Safety Evaluations are only mentioned, in Table 7-1 of DOE-STD-1189-2008 [6], as a typical action completed the end of preliminary design, without any specific mention of them in the standard's discussion of criticality safety or any specific format and content requirements in DOE orders or standards. However, this statement has been interpreted as a requirement for preparation of Preliminary Criticality Safety Evaluations by the end of preliminary design and the related incorporation of criticality safety evaluation results in hazard analyses, which was frequently missed in contractor attempts to implement DOE-STD-1189-2008 [8]. The lesson to be learned from this example is that SBD requirements should be clearly stated

and that supporting guidance should be provided in either SBD requirements document or supporting documents prepared as a part of the institutionalization of SBD

- **Complexity and Scope of Process.** The integration process mandated by DOE-STD-1189-2008 is complex, befitting the complexities of nuclear safety analysis and the interaction between nuclear safety measures and facility design. Safeguards measures, as a general rule, are simpler and less intrusive than safety measures. Therefore, the SBD process should be simpler than a safeguards analog of the nuclear safety process in DOE-STD-1189-2008. Moreover, the intimate relationships between safeguards accountability measures and State level material control and accounting (MC&A) measures and between safeguards containment and surveillance measures and State level physical Protection (PP) measures argue for an integrated approach addressing safeguards, MC&A, and PP. This integrated approach is much more likely to find acceptance within DOE than one that addresses only international safeguards, which do not apply to most DOE facilities [10].

Review of the process employed by DOE for the development and institutionalization of DOE-STD-1189-2008 identified the following good practice:

- **Early Involvement of Industry.** DOE-STD-1189-2008 was developed by a joint working group of DOE Headquarters staff (HSS staff under the leadership of Richard Englehart) and members of the Energy Facilities Contractors Group (EFCOG) Safety Analysis Working Group (under the leadership of Brad Evans) [11]. This approach helped ensure that the DOE-STD-1189-2008 requirements could be implemented cost effectively and provided a constituency for DOE-STD-1189-2008 within the DOE contractor community. The development and instutionalization of an SBD process for DOE contractors will be much more likely to succeed if it is developed employing a similar process.

Review of the process employed by DOE for the development and institutionalization of DOE-STD-1189-2008 identified the following opportunity for improvement:

- **Initial Focus on Designers/Safety Analysts Rather Than Project Managers.** One of the areas that led to problems with the institutionalization of DOE-STD-1189-2008 was that the requirements were considered design requirements. However, the focus of the DOE-STD-1189-2008 requirements is actually project management. Project managers, not designers, control the sequencing and scope of design activities and the membership of the project team and sub-teams like the SDIT. However, the DOE-STD-1189-2008 development team had great difficulty getting the attention of the EFCOG Project Management Working Group (PMWG) and other experienced project managers. The EFCOG PMWG considered DOE-STD-1189-2008 a design issue and had very little interest. When discussing this problem, Brad Evans commented, “Maybe we should have titled the standard ‘Integration of Safety into Project Management’.”[11] As a result, when the draft DOE-STD-1189-2008 was issued for review and comment it had very little input from experienced project managers and virtually no constituency in the DOE contractor project management community. As a result, the review, comment, and resolution process for DOE-STD-1189-2008 required nearly a full year and resulted in substantive changes to the process for integrating safety into design.

3.0 Conclusions and Recommendations

The review of the DOE experience in developing and implementing DOE-STD-1189-2008 led to the following recommendations for policy makers regarding the development and institutionalization of SBD within DOE. The priority, implementation difficulty, and recommended time frame for implementation (e.g., short term, intermediate term, or long term) is listed after each recommendation.

- SBD process requirements documents should be developed jointly by DOE staff and the DOE contractor community. The DOE contractor community can be most effectively engaged through the EFCOG working groups (i.e., the safeguards and security working group and the project management working group). It is most effective to provide these working groups with a broad outline of the need and let them fill in the details of the SBD process rather than to fund more detailed SBD process development by groups of safeguards experts. [High priority, easy to implement, near term]
- Despite the use of the term design in SBD, the primary audience for SBD requirements and guidance documents is the project managers who will implement SBD. If SBD is to be institutionalized within DOE, the DOE project management community must see its value. SBD documents for designers should focus on providing a "tool kit" of design approaches that would be acceptable to the IAEA (e.g., international documents analogous to DOE guides or NRC regulatory guides). [High priority, easy to implement, near term]
- The key element of SBD is the early establishment of expectations for integration of safeguards into design (at both the pre-conceptual and conceptual design stages) and the early negotiation of proposed safeguards approaches and measures between the project and the IAEA and State regulatory agency. The basic safeguard approaches and measures need to be agreed upon before the beginning of preliminary design. (That is, an agreed upon approach should be a requirement for CD-1 approval within the DOE project management process.) Implementation of this SBD element will drive projects to engage safeguards issues and employ safeguards subject matter experts (SMEs) early in the design process. Implementation of this SBD element will also require a change in the negotiation process and development of additional guidance by the IAEA and State regulatory agency. [High priority, difficult to implement, long term]
- The SBD requirements must permit tailoring of the SBD process to reflect safeguards risk, facility type and complexity, and the maturity of safeguards approaches for the specific design (e.g., whether the design is an evolution of an existing design for which effective safeguards measures have been developed or a revolutionary design requiring research and analysis to identify effective safeguards approaches and develop the requisite equipment). The universe of facilities being designed and constructed is large and a one-size-fits-all approach will not work. [High priority, difficult to implement, long term]
- Because of the small number of DOE facilities on the Eligible Facilities List and the even smaller number that are actually selected for IAEA safeguards, there is very little interest in a SBD process that addresses only IAEA safeguards within the DOE contractor

community. It is doubtful that such a process could be institutionalized in DOE. However, there is great interest in the DOE contractor community in an integrated process that addresses DOE requirements for special nuclear material protection (i.e., PP, MC&A, and security) in the design and construction of facilities. [10] International safeguards by design could piggy back on the development and implementation of such a process, sponsored by HSS or another DOE Headquarters organization, at little cost. [Intermediate priority, difficult to implement, intermediate term]

- The SBD process requirements documents should be structured to clearly identify all requirements and to identify the key project interfaces that affect design decisions related to safeguard approaches, measures, and performance. Technical guidance supporting the SBD process should be prepared by experienced safeguards SMEs. [1] [Intermediate priority, difficult to implement, long term]

4.0 Acknowledgements

The author gratefully acknowledges the support and guidance of Pacific Northwest National Laboratory and the Office of International Regimes and Agreements of the National Nuclear Security Administration.

5.0 References

1. Hockert, J., and Scott Vance, "Review and Analysis of Development of 'Safety by Design' Requirements, "PNNL-18848 Pacific Northwest National Laboratories, Richland, WA, October 2009.
2. Sell, C. Memorandum to Linton F. Brooks, David K. Garman, John S. Shaw, and Ingrid C. Kolb. "Integrating Safety into Design and Construction.", US Department of Energy, Washington D.C. December 5, 2005. Accessed at http://www.er.doe.gov/opa/PDF/0512%20Sell%20Memo.pdf.
3. Civil Engineering Research Foundation (CERF). *Independent Research Assessment of Project Management Factors Affecting Department of Energy Project Success*, CERFDOE Final Report-071204. Civil Engineering Research Foundation. 2004. Accessed at http://management.energy.gov/documents/CERFDOEFinalReport20071204.pdf
4. DOE Testimonies at Defense Nuclear Facilities Board Public Meeting and Hearing on Safety in Design. July 19, 2006. Accessed at http://www.hss.energy.gov/deprep/archive/safetyindesign/DOETestimonies_071906.pdf.
5. DOE Testimonies at Defense Nuclear Facilities Board Public Meeting Incorporation of Safety in Design and Construction. March 22, 2007, U.S. Department of Energy, Washington D.C. Accessed at http://www.hss.energy.gov/deprep/archive/safetyindesign/DOETestimonies_032207.pdf.
6. DOE-STD-1189-2008, *Integration of Safety into the Design Process*. March 2008, U.S. Department of Energy, Washington D.C. Accessed at http://www.hss.doe.gov/nuclearsafety/ns/techstds/standard/std1189/DOE-STD-1189-2008.pdf
7. *Annual Report To Congress - Department of Energy Activities Relating to the Defense Nuclear Facilities Safety Board - Calendar Year 2006*, U.S. Department of Energy, Washington D.C. Mar 2007. Accessed at http://www.hss.energy.gov/deprep/2007/TB07M14A.PDF.
8. Evans B, B Lowrie, and R Englehart. 2009. "DOE-STD-1189-2008 Integration of Safety info the Design Process -- An overview of the March 2008 Issued Standard and Lessons Learned." Presentation during training course at Energy Facilities Contractor Group (EFCOG) Safety Analysis Working Group (SAWG) Meeting, Las Vegas, NV, May 4, 2009, accessed at http://www.efcog.org/wg/sa/docs/DOE-STD-1189%20Integration%20of%20Safety%20into%20Design-5-04.pdf
9. *Systems Engineering Handbook—A Guide for System Life Cycle Processes and Activities. Version 3.1,* International Council on Systems Engineering (INCOSE). Seattle, Washington. Aug 2007.
10. Interview with Mr. Obie Amacker, Jr., Chairperson of the Energy Facilities Contractors Group (EFCOG) Safeguards and Security Working Group (SSWG) conducted at Pacific Northwest National Laboratory in May 2009.
11. Interviews with Mr. Brad Evans, Chairperson of the EFCOG Safety Analysis Working Group (SAWG), and Mr. Richard Englehart, at the EFCOG SAWG meeting in May 2009.

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by Battelle *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)
www.pnl.gov