U.S. DEPARTMENT OF ENERGY

PNNL-18848

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

Review and Analysis of Development of "Safety by Design" Requirements

J Hockert
SA Vance

October 2009

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-18848

Review and Analysis of Development of "Safety by Design" Requirements

J Hockert
SA Vance

October 2009

Prepared for
the Office of International Regimes and Agreements
National Nuclear Security Administration
under WBS 243.2.5 for Dunbar Lockwood, Team Leader

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

This report, the deliverable for Task 4 of the NA-243 Safeguards by Design Work Plan for Fiscal Year 2009, develops 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*. This experience was selected for study because of the similarity of the challenges of integrating safety and safeguards into the design process. Development of DOE-STD-1189-2008 began in January 2006 and the standard was issued for implementation in March 2008. The process was much more time consuming than originally anticipated and might not have come to fruition had senior DOE management been less committed to its success. Potentially valuable lessons can be learned from both the content and presentation of the integration approach in DOE-STD-1189-2008 and from the DOE experience in developing and implementing DOE-STD-1189-2008. These lessons are important because the institutionalization of SBD does not yet appear to have the level of senior management commitment afforded development and implementation of DOE-STD-1189-2008.

The key lessons for institutionalization of SBD to be learned from the DOE-STD-1189-2008 experience are:

- SBD process requirements documents should be developed jointly by DOE staff and the DOE contractor community.
- 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.
- The key element of SBD is the establishment of expectations for integration of safeguards into design prior to conceptual design (i.e., at the pre-conceptual design stage) and the negotiation of proposed safeguards approaches and measures between the project and the International Atomic Energy Agency (IAEA) and State regulatory agency by the end of conceptual design.
- 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.
- DOE projects have very little interest in a SBD process that addresses only IAEA safeguards; but they are very interested in an integrated process that addresses DOE requirements for special nuclear material protection. International safeguards by design could piggy back on the development and implementation of such a process, sponsored by Office of Health, Safety and Security (HSS) or another DOE Headquarters organization, at little cost.
- 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 subject matter experts (SMEs).

Acronyms and Abbreviations

CDNS	Chief of Defense Nuclear Safety
CD-1	Critical Decision 1
CNS	Chief of Nuclear Safety
CSDR	Conceptual Safety Design Report
DIQ	Design Information Questionnaire
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
EFCOG	Energy Facilities Contractors Group
HSS	Office of Health, Safety and Security
IAEA	International Atomic Energy Agency
MC&A	Material Control and Accountability
NNSA	National Nuclear Security Administration
NRC	Nuclear Regulatory Commission
PCSE	Preliminary Criticality Safety Evaluations
PMWG	Project Management Working Group
PP	Physical Protection
SBD	Safeguards By Design
SDIT	Safety Design Integration Team
SDS	Safety Design Strategy
SSC	Structures, Systems, and Components
SAWG	Safety Analysis Working Group
SSWG	Safeguards and Security Working Group

Contents

1.0 Introduction and Purpose

The Department of Energy (DOE) experience in developing and implementing DOE-STD-1189-2008, Integration of Safety into the Design Process (DOE-STD-1189-2008), can provide valuable insights to support the development and institutionalization of the Safeguards By Design (SBD) process. The purpose of this report is to develop the lessons to be learned for the institutionalization of SBD from the DOE experience with the institutionalization of DOE-STD-1189-2008. In order to identify these lessons learned, this report briefly describes: 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. This report constitutes the deliverable for Task 4 of the NA-243 Safeguards by Design Work Plan for Fiscal Year 2009. (Bjornard 2009)

The development and implementation of DOE-STD-1189-2008 was selected for study because of the similarity of the challenges of integrating safety and safeguards into the design process. Both nuclear safety and safeguards involve design features that often do not contribute directly to, and if not integrated in a timely fashion may actually impede, the production mission of the facility under development. Both safety and safeguards design approaches are largely driven by State level and international requirements. Failure to address either safety or safeguards requirements early in the design process can unnecessarily increase the costs and schedule duration of facility design and construction activities and can increase the risk that project budgets and milestones will not be met.

In this discussion, the term safeguards refers to those design measures incorporated to meet International Atomic Energy Agency (IAEA) requirements. Safety refers to those design measures incorporated to meet nuclear safety requirements imposed by State level regulators (e.g., 10 CFR 830). Security refers to those design measures incorporated to meet nuclear Material Control and Accountability (MC&A) and Physical Protection (PP) requirements imposed by State level regulators.

The report 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.*

2.0 Development and Purpose of DOE-STD-1189

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." (Sell 2005) The drivers for revision were analyses of the causes of cost and schedule overruns on large design and construction projects (CERF 2004) 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.[1] 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 (Sell 2005). 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 (DOE Testimonies 2006). 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 (DOE Testimonies 2007). 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. 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.[2] 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] The meeting agendas and participants' statements are available at http://www.hss.energy.gov/deprep/archive/safetyindesign.asp.

[2] For example the 2006 *Annual Report to Congress on DOE Activities Relating to the DNFSB* (U.S. Department of Energy 2007) 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."

3.0 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.

3.1 DOE-STD-1189 Content and Presentation

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.

3.1.1 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. The first is the rigor required in integration of safety into the design process, which is provided by the documented DOE Expectations for Safety-in-Design during the pre-conceptual design (DOE-STD-1189-2008). The second is the approach to developing the overall safety design basis for the project, which is provided by the documented Safety Design Strategy (SDS) and required to be developed as early in conceptual design as practicable.[1] This document is required to be approved by the DOE Safety Basis Approval Authority and the Federal Project Director, with the advice of the Chief of Nuclear Safety (CNS) or the Chief of Defense Nuclear Safety (CDNS), as appropriate.

The third important aspect of safety in design, where DOE-STD-1189-2008 mandated early DOE direction, is the review and approval of a newly required Conceptual Safety Design Report (CSDR), which is to provide preliminary identification of: 1) facility hazards, 2) the design measures proposed to eliminate or mitigate these hazards; 3) the proposed safety classification of the design measures; and 4) any exceptions taken to the safety design criteria imposed by 10 CFR 830, Nuclear Safety Management. This report must be formally approved, based upon a documented Conceptual Safety Validation Report as a part of the Critical Decision 1 (CD-1) approval to authorize project preliminary design.[2]

A recent DOE root cause analysis of significant contract and project management deficiencies (DOE 2008) identified the following as the most important root cause of project management deficiencies: "DOE often does not complete front-end planning (project requirements definition) to an appropriate

[1] The requirements for the SDS document are described in Section 2.3 and detailed in Appendix E of DOE-STD-1189-2008. DOE review and approval requirements for the SDS are discussed in Section 2.3 and Table 2-1 of DOE-STD-1189-2008.

[2] The requirements for the CSDR are summarized in Sections 3.2 and 4.2 and detailed in Appendix H of DOE-STD-1189-2008. The DOE review responsibilities and requirement for a CSVR are discussed in Table 2-1 of DOE-STD-1189-2008.

level before establishing project baselines." (DOE 2008) These new DOE-STD-1189-2008 requirements directly address this root cause by requiring that the DOE contractor project team, DOE safety basis reviewers in the field and at DOE headquarters, including the CNS/CDNS, and the federal integrated project team all agree on the basic safety approach and interpretation of DOE safety requirements for the project.

The application of a similar approach to SBD to DOE facilities subject to IAEA safeguards or to commercial facilities means that the IAEA will need to be able to review and approve safeguards design strategies, approaches, and measures much earlier in the design process. Currently, in the United States, the Design Information Questionnaire (DIQ) is submitted during final design (i.e., concurrent with the application for an NRC Construction Permit), and the Facility Attachment is negotiated during facility construction (i.e., information submitted to IAEA after the NRC License Application) (DOE 2008). Under an analogous SBD process, this early review would need to take place during conceptual design with continued negotiation and refinement throughout the remainder of the design and construction process. The IAEA would need to develop appropriate procedures and standards to specify the information requirements and review and approval process during each stage of the project. Because the interface between the typical project and the IAEA is through the State's regulatory process, the State regulator will also need to modify its regulatory approach to mandate the earlier submittal of information.

3.1.2 Mandatory Early Participation by Subject Matter Experts and Establishment of Integration Mechanism

Another significant change mandated by DOE-STD-1189-2008 is the formation of 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 overseeing the preparation of the nuclear safety deliverables and for other activities to ensure that safety is integrated into design (DOE-STD-1189-2008). This team is required to be established early in the conceptual design phase to prepare the SDS and CSDR. The requirement for these deliverables and the early establishment of the SDIT provide assurance that safety requirements and the strategies to meet them are developed early in the project. A similar approach could be employed as part of SBD. It is important to realize that requirements for submittal of safeguards design strategies, approaches, and measures early in the design process are necessary to ensure that the project is attentive to the recommendations of safeguards subject matter experts or an interdisciplinary team analogous to the SDIT. Interestingly one of the lessons learned from the DOE implementation of DOE-STD-1189-2008 was that safeguards and security subject matter experts were generally not included in the SDIT for nuclear facilities – even those possessing Category I quantities of Special Nuclear Material (Evans et al. 2009).

3.1.3 Mandatory Early Planning and Graded Approach

The requirements discussed above for early establishment of SBD expectations by IAEA and the regulator, for development of a safeguards design strategy and its early approval by the regulator and for early participation by subject matter experts, ensure that safeguards requirements are included early in project planning. This helps ensure that safeguards issues are identified and resolved early. Another important aspect of the DOE-STD-1189-2008 requirements is that the standard permits projects to use the SDS to tailor the application of the requirements for integration of safety into design based upon the

complexity and hazard of the facility.[1] This approach helps ensure that the DOE-STD-1189-2008 approach can be applied cost effectively across the broad spectrum of DOE facilities. It is important that the SBD process also be tailored so that it does not impose onerous requirements on projects for facilities where there are simple, standard safeguards approaches. Likewise, tailoring the SBD process could also ensure that adequate attention and effort is afforded projects developing facilities with difficult safeguard processes or revolutionary designs. Analogous to the DOE-STD-1189-2008 safety tailoring, the SBD tailoring approach proposed by the project should be reviewed and approved by the safeguards oversight organizations (i.e., the State's regulatory authority in consultation with the IAEA).

3.1.4 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 (DOE-STD-1189-2008). It also seeks to foster a risk management approach in 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 (Evans et al. 2009). It would be beneficial for SBD to incorporate a similar approach so that most of the surprises associated with implementation of safeguard measures later in the design were pleasant ones, resulting in cost and schedule savings. This is, however, an area where the DOE-STD-1189-2008 requirements have not been as effective as its authors intended (Evans et al. 2009). 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.

3.1.5 Identification of Key Project Interfaces That Affect 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. 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.

3.1.6 Identification of the End of Conceptual Design as the Key Point Where Basic Design Approaches and Parameters Need to Be Established

As presented above, in the discussion of early establishment of expectations and review of approach by owner/regulator, 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 (DOE-STD-1189-2008). A similar approach would be useful for SBD, because the decisions made during conceptual design commit as much as 80% of the total life-cycle costs (INCOSE 2007). As discussed above, 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

[1] The use of the SDS for tailoring is discussed in Sections 2.3 and 2.4.4 of DOE-STD-1189-2008.

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.

3.1.7 Clear Statement 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. An example is the requirement for Preliminary Criticality Safety Evaluations by the end of preliminary design and the related incorporation of criticality safety evaluation results in hazard analyses (Evans et al. 2009). This requirement is noted only as an expectation in Table 7-1 of DOE-STD-1189-2008 and is not specifically mentioned in Section 7.5 of DOE-STD-1189-2008. Section 7.5 states that "the NCS [Nuclear Criticality Safety] function must be represented on the project team and closely linked to the safety analysis effort from the earliest stages of project development. Criticality safety evaluations (CSE) must be integrated with the traditional safety analysis techniques to provide a comprehensive safety analysis. DOE has promulgated guidance for performing and documenting criticality safety evaluations in DOE-STD-3007-2007." (DOE-STD-1189-2008) However, neither DOE-STD-3007 nor DOE-STD-1189-2008 provides guidance on Preliminary Criticality Safety Evaluation preparation or the integration of NCS into safety analysis development. Therefore, it is not surprising that this nuance of DOE-STD-1189-2008 was cited as missed in application. 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.

3.1.8 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 MC&A measures and between safeguards containment and surveillance measures and State level 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.[1]

3.2 DOE-STD-1189 Development and Implementation

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

3.2.1 Early Involvement of "Industry"

DOE-STD-1189 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

[1] Interview with Mr. Obie Amacker, Jr., Chairperson of the EFCOG SSWG at Pacific Northwest National Laboratory in May 2009.

Group (EFCOG) Safety Analysis Working Group (under the leadership of Brad Evans).[1] 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. The EFCOG Safeguards and Security Working Group (SSWG) has expressed interest in working with DOE headquarters in developing an integrated SBD approach addressing safeguards, MC&A, and PP.[2] Therefore, it may be more productive to provide a DOE/EFCOG working group with a broad outline of a proposed SBD process and let them fill in the detail rather than having the inter-laboratory teams fully develop the SBD process for institutionalization. However, the joint DOE/EFCOG working group will make faster progress if the EFCOG effort is funded.[3]

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

3.2.2 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 a design issue and had very little interest. When asked about this problem, Brad Evans commented, "Maybe we should have titled the standard 'Integration of Safety into Project Management'."[4] As a result, when the draft DOE-STD-1189-2008 was issued for comment it had very little input from experienced project managers and virtually no constituency in the DOE project management community.

The review, comment, and resolution process for DOE-STD-1189-2008 required nearly a full year. The significant changes made during this process included:[5]

- Addition of a requirement for a DOE statement of safety-in-design expectations during pre-conceptual design;
- Provision of additional flexibility to tailor safety deliverables, the safety integration process, and risk and opportunity assessment process based upon the size, complexity, and hazard of the project;
- Decreased emphasis on activities during the transition from construction to operation; and

[1] 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.
[2] Interview with Obie Amacker, Jr.
[3] During the cited interview, Brad Evans noted that the EFCOG SAWG work on DOE-STD-1189 was an allowable overhead expense for the participating contractors but was not directly funded by DOE. As a result it was frequently the participant's lowest priority. He said that this significantly delayed the development of DOE-STD-1189.
[4] Interview with Brad Evans.
[5] The significant differences were identified through comparison of the review and comment draft of the standard available at http://www.hss.energy.gov/deprep/2007/TB07M29A.PDF with DOE-STD-1189-2008.

- Additional guidance for the interpretation of ANSI/ANS 2.26-2004, *Categorization of Nuclear Facility Structures, Systems and Components for Seismic Design*, a standard largely sponsored by DOE.[1]

With the exception of the last item, these are all additions that would likely have been incorporated in the initial draft of DOE-STD-1189-2008 had the project management community been engaged in its development. The lesson to be learned for SBD is that SBD is an approach to project management, not an approach to design. The audience for key SBD deliverables should be the project manager, not the designer. Although it may be useful to develop a safeguards design tool box that designers can use to develop safeguards measures that are cost effective and minimize impact on the overall project, the key features of SBD affect the way that projects are managed and executed. Thus the project management community must be involved in the development of SBD and must be sold on the process in order for it to be institutionalized.

[1] The need for extensive interpretative guidance in DOE-STD-1189-2008 to render useable a standard that was largely sponsored by DOE highlights the need to ensure that documents supporting the SBD process are of high quality, prepared by experienced, knowledgeable technical staff.

4.0 Conclusions and Recommendations for Policy Makers

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. 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. [Intermediate priority, difficult to implement, long term]

5.0 References

Bjornard, T. 2009. "NA-243 Safeguards by Design Work Plan for FY09 Includes NE Safeguards Campaign Sponsored Activities," Revision 1 (5-20-09)," attachment to e-mail from Trond Bjornard, subject "Final Version of SBD Workplan , with NE contributions", dated August 12, 2009.

Civil Engineering Research Foundation (CERF). 2004. *Independent Research Assessment of Project Management Factors Affecting Department of Energy Project Success*, CERFDOE Final Report-071204. Civil Engineering Research Foundation. Accessed at http://management.energy.gov/documents/CERFDOEFinalReport20071204.pdf

DOE-STD-1189-2008. 2008. *Integration of Safety into the Design Process*. DOE-STD-1189-2008, U.S. Department of Energy, Washington D.C.

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.

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.

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

International Council on Systems Engineering (INCOSE). Aug 2007. *Systems Engineering Handbook—A Guide for System Life Cycle Processes and Activities. Version 3.1*, INCOSE, Seattle, Washington.

Persinko, A. 1999. Memorandum to Mealane A. Galloway, "Summary of Meeting with Duke Cogema Stone and Webster to Discuss Technical Topics Associated with the Mixed Oxide Fuel Fabrication facility." December 20, 1999, U.S. Nuclear Regulatory Commission, Washington DC. Accessed at http://www.nrc.gov/materials/fuel-cycle-fac/mox/pdf/ml993630088.pdf.

Sell, C. 2005. Memorandum to Linton F. Brooks, David K. Garman, John S. Shaw, and Ingrid C. Kolb. "Integrating Safety into Design and Construction." December 5, 2005, US Department of Energy, Washington D.C. Accessed at http://www.er.doe.gov/opa/PDF/0512%20Sell%20Memo.pdf.

U.S. Department of Energy (DOE). Apr 2008. *Root Cause Analysis Contract and Project Management*. U.S. Department of Energy, Washington D.C. Accessed at http://www.management.energy.gov/documents/RCA_Report_FINAL_April_2008.pdf.

U.S. Department of Energy (DOE). Mar 2007. *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. Accessed at http://www.hss.energy.gov/deprep/2007/TB07M14A.PDF.

Distribution

No. of Copies

3 U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585
- Dunbar Lockwoood NA-243
- John Murphy NA-243
- George Pomeroy CF-20

1 Ed Wonder
U.S. Department of Energy
L'Enfant Plaza Building, NA-2431
1000 Independence Avenue
Washington, DC 20585

1 Scott Demuth
Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

1 Casey Durst
Durst Engineering & Consulting, Inc.
PO Box 944
Richland, WA 99352

1 Jim Morgan
InSolves Associates
1862 Shyville Road
Piketon, OH 45661

4 Idaho National Laboratory
2025 Fremont Avenue
Idaho Falls, ID 83415
- Robert Bean
- Trond Bjornard
- Fernando Gouveia
- Shauna Hoiland

1 John Hockert
XE Corporation
4611 Greene St., NW, Suite 307
Albuquerque, NM 87114

No. of Copies

5 **Local Distribution**
Pacific Northwest National Laboratory
- Obie Amacker, Jr. K8-02
- Deborah Dickman K8-14
- Brad Evans J2-50
- Carrie Mathews K8-14
- Scott Vance K8-14

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