INL/CON-09-16762
PREPRINT

Safeguards-by-Design: Early Integration of Physical Protection and Safeguardability into Design of Nuclear Facilities

Global 2009

T. Bjornard
R. Bean
S. DeMuth
P. Durst
M. Ehinger
M. Golay
D. Hebditch
J. Hockert
J. Morgan

September 2009

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Proceedings of Global 2009
Paris, France, September 6-11, 2009
Paper 9518

Safeguards-by-Design: Early Integration of Physical Protection and Safeguardability into Design of Nuclear Facilities

T. Bjornard[1], R. Bean[1], S. DeMuth[2], P. Durst[3], M. Ehinger[4], M. Golay[5] D. Hebditch[1], J. Hockert[6], J. Morgan [4]
1. Nuclear Energy Nonproliferation, Safeguards and Security, Idaho National Laboratory
Tel: 1-208-526-6328, Fax: 1-208-526-6239, E-mail: Trond.Bjornard@inl.gov
2. Los Alamos National Laboratory; 3. Durst Engineering & Consulting Inc.; 4. Oak Ridge National Laboratory; 5. Massachusetts Institute of Technology; 6. XE Corporation.

Abstract – *The application of a Safeguards-by-Design (SBD) process for new nuclear facilities has the potential to minimize proliferation and security risks as the use of nuclear energy expands worldwide. This paper defines a generic SBD process and its incorporation from early design phases into existing design / construction processes and develops a framework that can guide its institutionalization. SBD could be a basis for a new international norm and standard process for nuclear facility design. This work is part of the U.S. DOE's Next Generation Safeguards Initiative (NGSI), and is jointly sponsored by the Offices of Non-proliferation and Nuclear Energy.*

I. INTRODUCTION

The need exists to develop a simple, concise, formalized, and integrated approach for international safeguards as well as other nonproliferation and security considerations, and introduce this into facility design and construction management. Institutionalizing Safeguards-by-Design (ISBD) is the implementation of a structured approach by which international and national safeguards, physical security, and other nonproliferation objectives are fully integrated by means of a Safeguards-by-Design (SBD) process into the overall design and construction process for a nuclear facility; from initial planning through design, construction, and operation.

The overarching goal is the implementation of a new global standard for Safeguards-by-Design (SBD) to support the growth of nuclear power while reducing nuclear security risks. The term "institutionalizing" refers to adapting the SBD process and obtaining regulatory acceptance within the regimes of responsible State and international (IAEA) oversight organizations. The term, safeguards, is used broadly in this paper to denote national safeguards, physical protection, international safeguards and other proliferation barriers. Application of SBD in the facility design and construction effort is intended to provide early identification of safeguards requirements, intrinsic features, and options to optimize design, and to reduce impact to operation and minimize life-cycle cost.

The proposed SBD process manages interaction between safeguards design and the overall design process to progressively develop definition and analysis at each design phase and is expected to enhance the accuracy of project schedules and budget estimates. SBD has the potential to provide the greatest benefit for innovative designs (i.e. designs with limited experience on which to base the selection of major options, such as process flow-sheet, equipment selection, and facility layout) that require additional detailed development of the design approach. SBD has significant potential to improve control of cost and schedule risk during facility design and construction and reduce life-cycle cost associated with facility design, construction and operation. The basic ISBD approach is expected to be applicable, with adaptation, to all nuclear facilities regardless of the regulations or directives governing their design, construction, and operation. Although regulatory environments differ, the same basic decisions need to be made and the same basic management processes are required.

IA. Project Management of Design and Construction

Most projects requiring major financial commitments are managed using formal project management procedures and processes. In the nuclear industry, project management processes for facility design and construction are based upon regulations specific to disciplines required for project and execution including quality assurance, safety, and safeguards and security. Management of major projects is normally organized by project phases, associated with a logical maturing of broadly stated mission needs into well-defined requirements which are converted into design and construction of a facility meeting customer needs,[1] Fig 1.

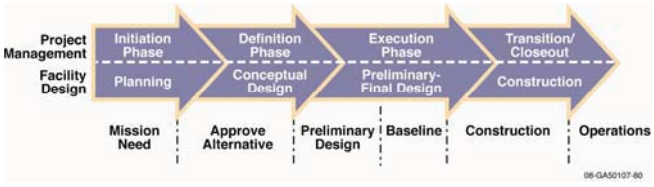

Fig. 1. Typical Phases of Project Management/Design

The project design team develops and evaluates approaches for a facility and processes that meet the project need. Feasible approaches are bounded by a set of requirements supporting the performance needed, materials and processes, areas such as environmental, safeguards and

safety requirements, and applicable regulations. The goal is to develop an optimal approach, in terms of cost and schedule objectives, for meeting all the requirements.

Systems engineering is a valuable tool for major projects, such as nuclear facilities.[2] It comprises technical and management processes, is an interdisciplinary field focusing on how complex engineering projects should be designed and managed, and is an effective way to manage complexity and change, and reduce cost and schedule risks. The conceptual design phase of a new system may often incur ~8% of the life-cycle cost, but the selected conceptual design commits ~70-80% of life-cycle cost.[2] This typical commitment of ten times greater cost is well known to the engineering profession and has stimulated responsive methodologies with increased emphasis on early definition of requirements, e.g. "front-end loading" (FEL). This illustrates the importance of the application of an SBD process where again the emphasis on early design involvement and definition is all important.

The SBD study, described below, examined design processes, best practices and lessons learned from major design projects, developments in the integration of nuclear safety, and project and systems engineering, in order to conceptualize the framework of essential elements for SBD. The ISBD framework consists of three "technical" pillars (requirements definition, design processes, and technology and methodology) standing on the foundation of institutionalization. All of these will be needed to support the achievement of a global SBD standard, see Fig. 2.

Fig. 2. High-level Framework to Institutionalize SBD

II. SAFEGUARDS REQUIREMENTS

Definition of requirements is the first technical pillar of the ISBD framework, see Fig. 2. Principal requirements for both the SBD process and for domestic and international safeguards are summarized below. All requirements necessary for the successful execution of SBD must be formalized, and demonstrated methodologies are needed to determine whether requirements are met by proposed designs. An assessment of the conceptual design to confirm that it meets, or has very high assurance of resulting in a final design that will meet, all requirements is essential prior to initiating later design phases. The same applies for the more detailed examination of adequacy in meeting the later, detailed, and comprehensive system requirements.

II.A. Process Performance Requirements for SBD Process

The objective for institutionalizing the SBD process is to provide a procedure by which international and national safeguards, physical security, and other nonproliferation objectives are fully integrated into the overall design and construction process for a nuclear facility, from initial planning throughout design and construction and with benefit to operation; with the goal of increasing the safeguardability, protectability and proliferation resistance of facilities. Although elements of SBD are incorporated in each phase of the project management process, the focus is on the early phases. High-level requirements for the SBD process itself were formulated as follows:

1. Develop a simple, concise, formalized, and integrated process for SBD that is beneficial to stakeholders
2. Develop the SBD process to be flexible, consistent with and to enhance the effectiveness of applicable domestic and international directives, e.g. NRC, DOE, IAEA
3. Provide a useful tool for the project manager responsible for design/construction of nuclear facilities
4. Base the SBD process on accepted project management, design, & systems engineering processes
5. Provide safeguards, security, & proliferation mitigation in the facility at minimum capability consistent with regulatory, etc., requirements and guidance
6. Mandate a concise set of project deliverables for safeguards design to demonstrate a systematic, comprehensive, auditable, and transparent project design
7. Develop phased safeguards effectiveness reports to facilitate dialog with and acceptance by sponsors
8. Initiate safeguards design activities in the pre-conceptual planning phase through the establishment of a safeguards design team
9. Use systems engineering to integrate operability, safety, security, safeguardability, and proliferation resistance into the facility design
10. Provide early identification of intrinsic design features that enhance safeguards, security, or proliferation barriers, or assist implementation of extrinsic measures
11. Mandate use of life-cycle cost (LCC) analysis as a criterion for capital expenditure decisions between intrinsic (early) and extrinsic (later) design alternatives

II.B. Prescriptive Requirements for the SBD process

The SBD process must comply with current regulations, agreements, directives, etc., (e.g. NRC, DOE, CFR, IAEA) for the nuclear fuel cycle affecting safeguards. The facility, as designed, constructed, and operated must also comply with these and other requirements. National and international, safeguards and security often covers such areas as:

1. Physical Protection
2. Material Control and Accountability (MC&A)
3. Cyber Security

Several other areas are being studied, e.g. by Gen IV – GIF[3] and IAEA INPRO[4]. Although still unaccepted internationally in terms of requirements or methodologies for assessing designs, studies are progressing regarding:

4. Proliferation Resistance (PR)
5. Safeguardability (one important aspect of PR)

The high-level structure of U.S. obligations, federal regulations and facility design interfaces with the IAEA under the Nuclear Non-Proliferation Treaty (NPT), are shown in Fig. 3. The boxes under "International Oversight" summarize high-level steps during facility design, construction, and operation.

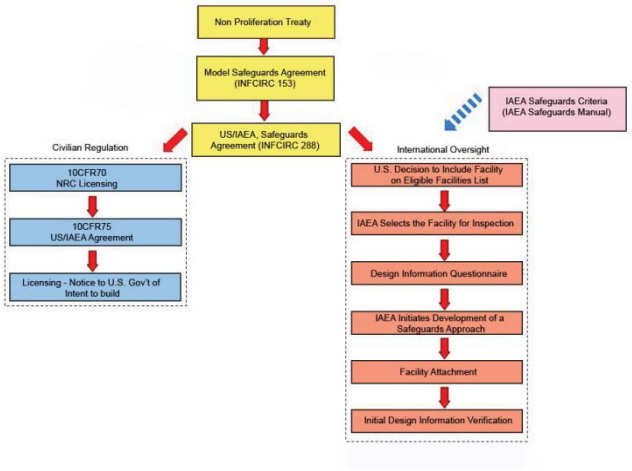

Fig. 3. U.S. Obligations and Interfaces with IAEA

The four main elements of the IAEA process to apply a facility-specific safeguards approach after the Agency is notified of the intent to build a new facility (in the U.S. by addition to the Eligible Facilities List [EFL]) are:

1. Receipt by IAEA of the completed Design Information Questionnaire (DIQ) from the State authority
2. Initiate the process of developing a Facility Safeguards Approach by the IAEA
3. Negotiation of the Facility Attachment by the IAEA with the State authority
4. Design information verification (DIV) by IAEA during construction and throughout the life of the facility

During several decades of facility design, construction, operation, and decommissioning, many IAEA safeguards requirements apply including that the facility enables:

1. Defined Material Balance Areas
2. Key Measurement Points for measuring the flow and inventory of nuclear material
3. Defined Strategic Points for the application of containment/surveillance and other verification activities
4. Nuclear Material Accountancy based on facility operating records and State reports
5. An annual Physical Inventory Taking and Verification
6. Verification of domestic and international transfers of nuclear material
7. Accounting process permitting IAEA to perform a statistical evaluation of the nuclear material balance
8. Routine Interim Inventory Verifications for timely detection of possible diversion of nuclear material
9. Verification of facility design information (safeguards)
10. Verification of facility operator's measurement system

III. EXAMPLE OF DESIGN/CONSTRUCTION MANAGEMENT WITH SBD FOR SSAC

Design processes for SBD, sections III and IV of this paper, form the second technical pillar of the ISBD framework, see Fig. 2. SBD is a process that must be integrated with the project management, engineering design (especially including safety) and systems engineering process utilized for the design and construction of nuclear facilities. Countries, party to the NPT, conclude a comprehensive safeguards agreement with the IAEA to cover the construction and operation of their nuclear facilities. The IAEA's experience in safeguards implementation is used in conjunction with the capabilities of the State system of accounting for and control of nuclear material (SSAC) in developing the safeguards agreement. In this context and as an example for evaluating the international application of safeguards, the SBD process was tested by applying the U.S. DOE regulatory environment. Significant DOE directives included DOE-STD-1189-2008, Integration of Safety Into the Design Process, and DOE G 413.3-3, Safeguards and Security for Program and Project Management, which provide guidance for integration of safety with security during the design process. The DOE directive system was chosen for this initial study due its completeness and detailed structure.

A workshop study proposed a SBD process within the DOE design and construction management process that addessed:

1. Prescriptive requirements of the DOE directives system for design and construction management for the acquisition of facilities (capital assets)
2. Prescriptive requirements of the IAEA since the U.S. has voluntarily entered into obligations for application of international safeguards to fuel cycle facilities
3. Performance requirements developed by the SBD study for the SBD process (these also call out some regulatory requirements)

The study generated a single proposed process covering DOE domestic regulatory requirements and international (IAEA) safeguards. The study was performed in two stages: first, developing a process using DOE domestic requirements and SBD performance requirements only, and second, modifying the first results to integrate the additional effects of incorporating international (IAEA) requirements. The step-wise approach simplified the study and facilitated its visual representation by means of two series of detailed flowcharts.

III.A. Proposed SBD Process in U.S. DOE Structure

In this example, which utilizes a systematic series of steps directed to fully integrate international and national safeguards, physical security, and proliferation risk reduction into the design process for nuclear facilities, the proposed SBD process is structured to the phases of the DOE project management and design process with the goal of increasing the safeguardability, protectability, and proliferation resistance of facilities. Critical decision (CD) points are part of this gated process, which specifies that particular requirements need to be met and approval must be achieved to continue with the project. The phases for a DOE project are illustrated in Figs. 1 and 6. The DOE acquisition process defines the project definition phase, between CD-0 and CD-1, as conceptual design. The project execution phase between CD-1 and CD-2 is defined as preliminary design. By the end of this phase, the project is to have a sufficiently well-defined estimate of cost and schedule and set of technical requirements to serve as a technical baseline for the remainder of the project. The project execution phase between CD-2 and CD-3 is defined as final design and produces a design that can be used for construction. Design activities during the construction phase of project execution (between CD-3 and CD-4) are limited to those necessary to resolve constructability issues and verify that field changes maintain conformance with design requirements.

During conceptual design, the SBD process creates an SBD team to assist the SBD team lead. The SBD team incorporates safeguards requirements into the Project Functional and Operational Requirements. This information is integrated into the SBD Conceptual Phase design activities, which utilize an iterative graded process called the SBD design loop, see Fig. 4. This loop is also used in later design phases. The internal design steps may be invoked or deferred as needed whilst the design matures. The design that is passed to the SBD team is modified and reviewed internally until the team is satisfied that it meets the established requirements. Design will then exit the SBD Design Loop to enter a Project Design Review process, conducted by project peers, primarily directed at ensuring that the safeguards design is in alignment with the overall project design.

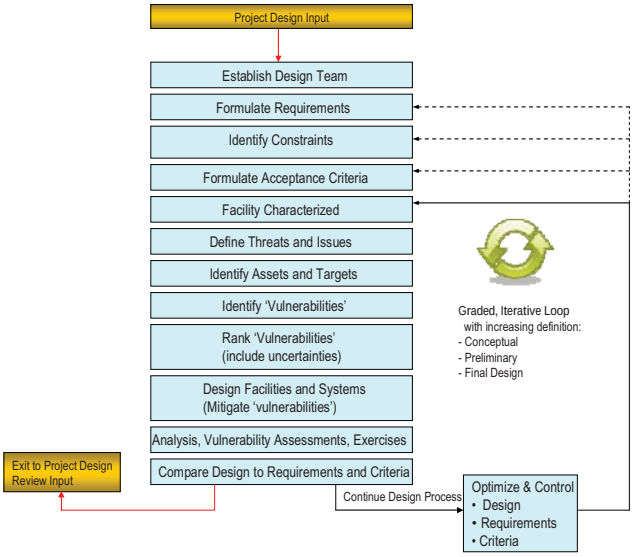

Fig. 4. SBD Design Loop.

These process steps for safeguards interact with the DOE Project Management structure. As an example, the flowsheet for the conceptual phase is shown in Fig. 5.

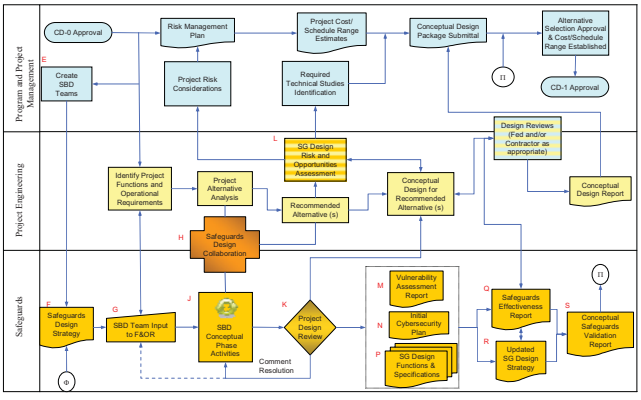

Fig. 5. SBD Process for DOE Domestic System – Conceptual Phase- Steps 6-17 of Table I

In summary, there are 41 main steps making up the proposed SBD process in support of DOE domestic requirements for facility acquisition, see Table I for those

in the conceptual design phase. The three iterations of design (definition, preliminary, and final) comprise cycles of safeguards activities: design, review, risk/opportunity assessment, vulnerability assessment, cyber security plan, specification development, effectiveness review, strategy development, and stakeholder response. There are also startup (pre-conceptual planning) and closeout phases (construction). The complexity is comparable to existing methodology for integration of safety into the design process.[1,3]

Table I
Steps in SBD Process for Domestic Requirements

#	SBD PROCESS STEPS
CD-0	**Definition Phase – Conceptual Design**
6.	Generate and document Safeguards Design Strategy
7.	SBD Team Input to Design Requirements
8.	Participation in facility conceptual phase design studies
9.	Perform SBD conceptual design activities within SBD Team
10.	Participate in project, peer reviews of facility conceptual phase design
11.	Perform a Safeguards Risk & Opportunities Assessment
12.	Conduct Vulnerability Assessment
13.	Document the Initial Cyber Security Plan
14.	Develop Safeguards Design Functions & Specifications
15.	Provide Safeguards Effectiveness Report
16.	Update Safeguards Design Strategy
17.	Seek DOE to provide Conceptual Phase Safeguards Validation Report

III.B. Proposed SBD Process with Integration of International Safeguards and U.S. DOE Structure

IAEA requirements are used to develop the second stage of the SBD process for domestic and international safeguards. The four principal elements for instituting IAEA safeguards—i.e., DIQ, safeguards approach, facility attachment, and DIV, must be integrated into the State acquisition system, see Fig. 6, for the case of U.S. DOE. The double-ended arrow shows that the DIQ is started as early as possible after CD-0. The remaining IAEA activities are associated with certain critical decision points within the DOE framework, but are also dependent on the completion of previous IAEA activities. The dashed arrows illustrate the ongoing relationship between the IAEA and the owner/operator of the nuclear facility into the operations phase. Submission of the DIQ is the clear responsibility of the facility owner/operator, gradating to joint negotiation of the facility attachment and separate responsibility of the IAEA for the safeguards approach and DIV. However, all these depend on mutual cooperation in order to be effective.

The IAEA safeguards points of interaction with DOE Program and Project Management, Project Engineering and Safeguards were developed using a second set of detailed flowcharts. The two sets show all steps for the SBD process with combined DOE domestic regulatory directives and international safeguards. In conclusion, some 14 additional, main steps are incorporated into the

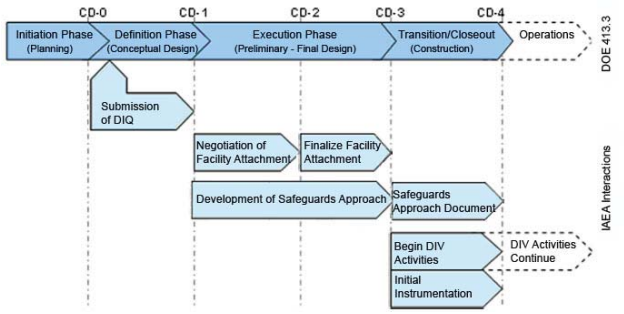

Fig. 6. Integration of IAEA Safeguards Activities within DOE Acquisition System

SBD process to account for the IAEA safeguards requirements in support of DOE facility acquisition. Again, there are iterations of the three later design phases (conceptual, preliminary, and final) and lastly facility construction, transition, startup, and closeout. The SBD process steps created to meet international requirements are listed in Table II. These process steps complete the SBD process for integration with DOE Program and Project Management and Project Engineering.

Table II
Steps in SBD Process for International Requirements

#	SBD Process Steps
CD-0	**Definition Phase – Conceptual Design**
1.	Determination whether to place planned facility on EFL
2.	Notify IAEA of Intent for Facility
3.	Potential early start to preparation of DIQ
4.	Potential early transmission of DIQ to IAEA
CD-1	**Execution Phase – Preliminary Design**
5.	Prepare Design Information Questionnaire
6.	Transmit Design Information Questionnaire to IAEA
7.	Develop Facility Attachment
8.	Negotiate Facility Attachment information with IAEA
9.	Finalize IAEA Facility Attachment Input to physical plant
CD-2	**Execution Phase – Final Design**
10.	Final Facility Attachment input to IAEA
11.	Submission of Program Requirements Document (PRD)for construction/ projects being executed by NNSA
CD-3	**Transition/Closeout - Construction**
12.	IAEA undertakes Design Information Verification activities
13.	Delivery of IAEA safeguards equipment to facility
14.	Installation of IAEA safeguards equipment in facility

III.C. Complete SBD Process for DOE Environment

The study generated an integrated SBD process covering DOE domestic regulatory directives and

international (IAEA) safeguards for a DOE design and construction management project. It comprises 55 process steps. This approach tested the adaptability of the SBD process in a structured environment, i.e., the DOE system for acquisition of capital assets. Although new directives have not been drafted for use of SBD within the DOE acquisition system, the SBD process is considered to be sufficiently developed to be tested on a pilot scale for an actual DOE project. This pilot scale exercise would evaluate and improve process viability and help determine the best way to effect institutionalization within the DOE regulatory structure. The methodology used is recommended for the shaping of the SBD process to other design and construction environments in the U.S. such as that for commercial facilities regulated by the NRC.

The two-stage approach also suits institutionalization that addresses specifically the integration with international safeguards, since the DOE regulatory system is an example of what the IAEA calls the SSAC of nuclear material.

IV. GENERIC PROCESS FOR SBD

After the experience of integrating the SBD process with that for DOE design and construction management, the SBD essentials were quickly identified in the form of a generic process. Benefits include recognizing principles, supporting testing, and facilitating the use of SBD within other domestic and foreign regulatory environments. Key elements include:

Planning Phase

- Mandated participation of safeguards (SG) subject matter expert(s) in concept development
- Identification of facility SG categorization and associated requirements as early as practicable
- Identification of applicable international, national, and organizational SG requirements and separation of prescriptive and performance based SG requirements
- Formalized, graded SBD process based on: (1) SG categorization, (2) methodology for SG effectiveness
- Prescriptive requirements provided to project systems engineering process to be incorporated into the design
- Conceptual strategies for meeting performance requirements: (1) “off the shelf” SG measures, (2) R&D to enhance existing measures/develop new, and (3) design changes to enhance protectability and safeguardability (intrinsic), (4) unclassified design requirements to implement conceptual strategies, etc
- Phased analyses demonstrating, at appropriate level of assurance, that the conceptual strategies will meet the SG performance requirements
- Identification and configuration management of the SG “envelope” (set of intrinsic features and associated requirements for meeting prescriptive and performance requirements) to ensure that SG capabilities and compliance are maintained as the design progresses
- Preliminary analysis of project risk associated with conceptual strategies for meeting SG performance requirements, including risk mitigation strategies
- Documentation of SG categorization, requirements, conceptual strategies for meeting performance requirements, SG envelope, & project risk assessment with subsequent review by owners and stakeholders to obtain approval of approach, risks and strategies
- SBD elements included in approval of project plans authorizing the project to proceed to the next phase

Conceptual and Final Design Phases

- Mandated participation of SG subject matter experts in design development. Provide leadership in SG design and review all changes affecting SG envelope
- Validation of SG categorization and applicable requirements as design matures
- Refinement of strategies for meeting SG performance requirements as design matures. Development of next lower-level functional requirements based on refined strategies and maturing design. Associated refinement of SG envelope and increased formality of configuration management
- Refinement of analyses showing SG strategies meet developing SG performance requirements. Refinement reflects maturing design, reduced uncertainties of SG measures and design details, and use of more sophisticated analytical approaches. Risk-informed methods for assessing and mitigating vulnerabilities are preferred
- Development of analysis of project risk of conceptual strategies for meeting SG performance requirements, refinement of risk mitigation strategies from maturing design and R&D. Implementation of risk management strategies as required
- Continued systems engineering and design to meet prescriptive SG requirements and to implement strategies for meeting SG performance requirements
- Completed documentation of SG categorization, applicable requirements, SG strategies developed for meeting performance requirements, analyses showing adequacy of the SG strategies, definition of the SG envelope, and project risk assessment. Approval of documentation as part of construction authorization
- For facilities on the Eligible Facilities List (EFL), the designer collaborates with IAEA concerning DIQ as early as practicable during design phase. The Facility Attachment is jointly negotiated and completed during this phase

Construction Phase(s)

- Mandated participation of SG subject matter experts in review of field and design changes affecting SG envelope
- Development of analyses showing that SG strategies meet SG requirements. Development of analyses reflects field design changes, demonstrated capabilities of SG measures, and detailed as-built configuration
- Continuing systems engineering and quality assurance validation activities, including performance validation that as-built design meets SG requirements as construction proceeds. SG acceptance reviews and validation at end of construction prior to operations
- Development of plans, policies, and procedures to implement strategies for meeting SG performance requirements in operation, including minor strategy modifications to address operational constraints
- Implementation of project risk management strategies associated with meeting SG requirements, as required
- Completed documentation of SG categorization, applicable requirements, conceptual strategies developed for meeting performance requirements, analyses demonstrating adequacy of the SG strategies, definition of the SG envelop, project risk assessment, and SG validation activities. Approval of documents as prerequisite for facility commissioning for operation
- At end of construction activities, documentation also includes (1) the results of SG acceptance reviews and validation and (2) the SG commitment documents (e.g. security plans, material control and accountability plans) and security approval of facility operation
- For facilities subject to IAEA SG, IAEA design verification activities are commenced, and installation of IAEA SG equipment is completed. At end of construction, all equipment needed for implementation of IAEA SG is to be installed, tested, & accepted. DIV continues throughout the facility's operational lifetime

IV.A. Key Features of the Generic SBD Process

In summary, the key features are:

1. Early involvement of SBD team in the design effort
2. Early identification of safeguards requirements and intrinsic features that will benefit the design
3. Closer integration of safeguards with project design, leading to improved cost estimates and schedules
4. A clear and simple interaction plan between safeguards and the formal design process that identifies required activities and their timeline and provides detail and analyses at each phase of the design cycle
5. Specific requirements for owner/stakeholder approval of SG design approaches and associated risks at key decision points
6. Flexibility to incorporate all regulatory requirements into the design of nuclear facilities

These key features help ensure cost-effective integration of safeguards into design in a manner that controls and minimizes the project risks associated with meeting national and international safeguards requirements.

IV. B. Development of the Generic SBD Process

The generic SBD process, shown in this section, documents the process essentials in a generic design and construction project. Some further work in this area may examine a minimal set of baseline safeguards performance requirements, as seen within the physical protection, MC&A, and international safeguard requirements of NNSA, DOE, NRC, and IAEA, together with those established by other nations (e.g., France, Japan, RF and UK). Within this basic requirement set, the minimal process steps for SBD and their optimal phasing could be established. These SBD activities may then be integrated more easily within a generic project management sequence that might incorporate a variable number of hold points (critical decisions) and could form a single path or comprise multiple parallel paths. This may bring increased flexibility to institutionalize SBD within the framework of any of these safeguards oversight regimes. The recommended refinement of the generic process could occur during future work with the IAEA toward developing a global standard for SBD.

V. SUPPORTING TECHNOLOGY & METHODOLOGY

Technology and methodology form the third technical pillar of the ISBD framework, see Fig. 2. This area includes methodologies for assessing facility designs for compliance with design requirements. Some of these methodologies are under development and not yet well accepted by regulators and industry. The SBD process has the flexibility to enable parallel testing and methodology development. Links to NGSI studies, related work at the IAEA, needs for and progress with technical solutions, guiding principles, and a summary of best practices and lessons learned relevant to SBD, are discussed below.

Proliferation Resistance and Safeguardability

No nuclear energy system can be made proliferation proof; however, different systems can present varying degrees of proliferation risk stemming from the combined application of international safeguards plus other proliferation barriers. The incorporation of these other proliferation barriers in facility and process design can be readily dealt with in the

proposed SBD process, provided relevant requirements are articulated, formalized, and included in the design process. Methodologies under development worldwide include the PR-PP Methodology[4] of the Generation IV International Forum and the INPRO approach[5] developed by an IAEA-led team. The two are currently undergoing joint review and coordination.

Needs for Development of Methodologies

Supporting methodology development is required since methods are not formally accepted, domestically or internationally, for assessment of proliferation barriers and safeguardability of nuclear facilities as needed for application of the SBD process. Without accepted methodologies, the effectiveness of implementing safeguards requirements cannot be quantitatively evaluated. No strong case can be made for safeguards-driven selection of fundamental facility design options such as fuel cycle, process, flowsheet, and remote maintenance philosophy, and SBD has little influence on the selection of facility alternatives unless they are cost neutral. Essentially, SBD in the physical protection area is already feasible using vulnerability assessment based on the design basis threat (DBT), although there are initiatives to evolve to risk-informed assessment. Some parties perceive SBD to be feasible within the international safeguards arena once the facility layout, process, and major equipment have been adopted, e.g., recent reprocessing facilities. However, the latter removes the full potential benefit of SBD. For gas centrifuge enrichment plants with strong commercial confidentiality concerns, early conceptual design for online safeguards instrumentation and other Material Balance Areas monitoring in cascade halls is particularly difficult to establish without well-justified proliferation barrier requirements. However, based on the lessons learned from the earlier formalization and culture shift for safety-in-design, full regulatory and industrial acceptance of SBD will require a concerted effort to demonstrate that SBD benefits not only safeguardability, but also project cost and schedule reliability through pilot testing of the process. Simple replication of the safety-in-design approach for SBD is not expected to be possible due to differing performance and prescriptive requirements and psychology, human performance, and limitations in fault tree treatment for risk assessment. The current SBD approach is expected to accommodate most new proliferation resistance requirements and evaluation methodologies.

High-level performance requirements for the SBD process were formulated in this study but found to be mainly qualitative in nature, which contrasts with lower-level prescriptive requirements, e.g., DOE physical protection directives. More detailed and semi-quantitative requirements may be needed for SBD process optimization.

SBD and NGSI Roadmap

The demonstration and institutionalizing of the SBD process is a fundamental element of the Next Generation Safeguards Initiative prepared by the U.S. DOE National Nuclear Security Administration, Office of NA-24. Its objectives include demonstration and institutionalization of SBD, development of associated guidelines, requirements and best practices, and the demonstration of SBD at a new nuclear facility in the US or in a foreign country.

SBD and Related Work at IAEA

In October 2008, the IAEA held a "Workshop on Facility Design and Plant Operation Features that facilitate the Implementation of IAEA Safeguards" where safeguards-by-design was a major topic. It was found that the definition and purpose of SBD processes as seen by NNSA, DOE National Laboratories and the international community were complementary and underscored the need and value of an SBD process for ensuring that the design and construction of new nuclear facilities is efficient and that these designs incorporate the necessary features for the effective application of nuclear safeguards throughout the world.[6] SBD will also facilitate various IAEA goals and objectives, such as: (1) Enhancing safeguardability in new nuclear facilities; (2) Reducing the time and cost for the inspectors' physical presence at facilities; (3) Incorporating process monitoring into the safeguarding of nuclear facilities; and (4) Sharing equipment and instrumentation between the operator and the IAEA.

Safeguards-by-Design Guiding Principles

To apply the SBD process to a particular nuclear facility design, experience with project management, systems engineering, and safeguards leads to a preliminary set of guidelines or principles. These guiding principles apply to all nuclear facility design efforts and serve to enhance the consistency with which SBD provides benefit to any given project. A preliminary set of guiding principles for applying Safeguards-by-Design was developed.

Examination of Best Practices and Lessons Learned

Six major nuclear fuel cycle projects were studied as an early part of the development of the ISBD framework and SBD process. Experiences from the design of the Rokkasho Reprocessing Plant and the Mixed Oxide Fuel Fabrication Facility, the development of Unclassified (UCNI) Design Requirements for Safeguards at a U.S. nuclear facility, the patterns of safeguards integration at

U.S nuclear facilities, and the leak of dissolver product liquor at the Sellafield Thermal Oxide Reprocessing Plant were examined. Best practices and lessons learned from these studies helped shape the SBD study.

VI. INSTITUTIONALIZING SBD

VI.A. Outreach

Institutionalization is the foundation supporting and implementing the three technical pillars of the ISBD framework, see Fig. 2. The entire ISBD framework directly supports the goals of the NNSA NGSI in its international safeguards aim of establishing a new global standard for effective application of SBD. A strategy is needed to transfer the ISBD framework and SBD process into international safeguards activities under NNSA and IAEA participation. Technical collaboration activities potentially include training, shared methodology testing and document drafting.

U.S. collaboration took place with the IAEA under its Facility Design Facilitating IAEA Safeguards Workshop, which took place in October 2008, with international participation for identifying design features, policy, and process, that enhance safeguardability. This complements the activities proposed under the IAEA International Symposium (IAEA, April 2009) on "Nuclear Security: Safety, Security and Safeguards Interfaces" to determine how the "3S concept" can best be implemented.[6] Further support is also needed for the IAEA's Facility Design initiative. Other work includes translation of the SBD process into a generic model framework that could serve as a new global standard for SBD, possibly in conjunction with the IAEA's own project. Domestic and international recognition for the ISBD framework and SBD process should be raised using publications and workshops to promote awareness, understanding and acceptance.

The international outreach capabilities of NNSA, Office of Export Control Policy and Cooperation (NA-242), and its current bilateral and multilateral cooperation programs, may be leveraged to promote the SBD approach in States that are pursuing the utilization of nuclear energy. This would be analogous to the current outreach effort supporting export controls and would target emerging nuclear States. Other possibilities include participation in an international facility design project for demonstration of SBD, and collaboration with international professional organizations, e.g., American Society of Mechanical Engineers, and International Standards Organization.

Sponsor review has started and is likely to continue. Wider stakeholder review is planned. The list of stakeholders includes the NNSA, DOE Offices of Nuclear Energy, and Health, Safety and Security; Department of State, the DOE-STD-1189-2008 pilot teams with the Y-12 project at Oak Ridge and the Idaho Waste Treatment Project, facility design and construction managers and users of DOE Order 413.3A, design team members of related disciplines (e.g., safety), and various subject matter experts. An expert group provided by the Energy Facilities Contractor Group (EFCOG) drafted DOE STD-1189-2008. The Defense Nuclear Facilities Safety Board has a statutory role concerning safety of DOE facilities. NNSA and Department of State have primary positions in the implementation of the Voluntary Offer Agreement (VOA) and AP[7] with the IAEA.

VI.B. Commercial and DOE Facilities

A strategy is needed to apply the SBD process to the design of commercial facilities regulated by the NRC. Uranium enrichment facilities may be the most safeguards-significant new commercial facilities in the near term in the United States, as well as around the world. Two such facilities are under construction and two more NRC applications are expected: LES National Enrichment Facility gas centrifuge plant in New Mexico, USEC American Centrifuge Plant in Ohio, planned AREVA gas centrifuge enrichment plant in Idaho and planned GE-H application for a full-scale laser (SILEX) uranium enrichment facility in North Carolina. AREVA has indicated its intent to proceed eventually with a nuclear fuel recycling facility in the United States. NRC has already issued the construction permit for the DOE Mixed Oxide Fuel Fabrication Facility (MFFF) and the licensing of operation is under review. The MFFF project team may be willing to review the SBD process. There are potential commercial deployment facilities such as the consolidated fuel treatment center. The SBD process needs to be applied to actual facility projects to improve methodology, provide staff familiarization, and demonstrate benefits for stakeholders.

In 2008, DOE and NRC delivered to Congress the Next Generation Nuclear Plant (NGNP) Licensing Strategy Report describing the licensing approach for an advanced reactor design by 2017.[8] This project may form a valuable pilot test bed with effective SBD application for an advanced nuclear energy facility. SBD participation is also sought in a DOE project where implementation of DOE STD-1189-2008, is being examined. Previously, DOE has employed pilot testing of Safety-in-Design in the Idaho National Laboratory Waste Treatment Project and the Y-12 Uranium Processing Facility at Oak Ridge.

VII. CONCLUSIONS

1. A conceptual framework for Institutionalizing Safeguards-by-Design (ISBD) has been developed for formalizing the development and deployment of the SBD process. These support the NGSI and key IAEA safeguards objectives, and may be useful internationally in establishing a high-level global standard for support of nuclear facility design.

2. The framework includes requirements definition, design processes, technology and methodology, and institutionalization activities. It uses these to increase the effectiveness and efficiency of the safeguards design process as part of nuclear facility design, construction, and operation.

3. The framework is expected to be readily adaptable to almost all regulatory, project management, and engineering environments and is applicable to a wide range of nuclear facilities; although much work remains to achieve a new global safeguards standard.

4. A generic SBD process and the means for its incorporation into existing facility design and construction processes have been developed and could ultimately form the basis for a new international norm and standardized process for nuclear facility design.

5. The proposed SBD process can be applied beneficially today, using existing requirements and methodologies. The results obtained are likely to be improved as more of the SBD framework is used and the designer's methodological toolkit is expanded. The development of design principles, guidelines, and best practices is seen as a valuable near term addition.

6. Strong evidence of value of the SBD process is likely to be required before promulgation under regulatory directives or adoption under industry initiatives. This may be best achieved through SBD pilot testing.

7. Key features of the proposed SBD process include: initiation of safeguards design activities in the pre-conceptual planning phase, early appointment of an SBD team, timely definition of requirements, participation in facility design options analysis in the conceptual design phase to enhance intrinsic features, definition of new deliverables akin to safety reports, assisting the project director in ensuring safeguards requirements are met, and formal communication of risks and management strategies to decrease the cost and schedule uncertainties.

8. The principal focus of the proposed SBD process is on the early inclusion of requirements, and the early identification of beneficial, e.g. intrinsic, design features. Modern design practices are increasingly front end loaded, and the possibility to significantly influence major design features, such as process selection and plant layout, largely ends with conceptual design.

9. There is a need for continuing development of supporting methodologies for the assessment of areas such as safeguardability and physical protection of nuclear facilities so that safeguards implementation can be more rigorously evaluated, and safeguards-driven changes to basic design options at the conceptual design stage may be better evaluated by the project management and client.

10. The authors believe that successful implementation of the SBD process will support the growth of nuclear energy while reducing proliferation and security risks.

ACKNOWLEDGMENTS

The authors gratefully acknowledge support by the National Nuclear Security Administration under the U.S. DOE's Next Generation Safeguards Initiative, and by the DOE's Office of Nuclear Energy, Advanced Fuel Cycle Initiative, Safeguards Campaign. They also acknowledge permission to publish from the DOE.

REFERENCES

1. DOE Order 413.3A, Program and Project Management for the Acquisition of Capital Assets, 07/28/2006.

2. INCOSE, Systems Engineering Handbook, Guide for System Life Cycle Processes and Activities, Version 3.1, August 2007.

3. DOE Standard STD-1189-2008, Integration of Safety into the Design Process, March 2008.

4. Gen IV International Forum, PR-PP Expert Group, "Evaluation Methodology for Proliferation Resistance and Physical Protection, Rev. 5," GIF/PRPPWG/2006/005, OECD, November 30, 2006.

5. IAEA, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual - Proliferation Resistance, Vol. 5, Final Report of Phase 1, 16-07-2007.

6. R.S. Bean, T.A. Bjornard, D.J. Hebditch, Safeguards-by-Design: An Element of 3S Integration, International Symposium on Nuclear Safety, IAEA, Vienna, Austria, April, 2009

7. Manual for Implementation of the Voluntary Offer Safeguards Agreement and Additional Protocol with the IAEA, DOE M 142.2-1, 9-4-08.

8. DOE-NRC, Next Generation Nuclear Plant Licensing Strategy, Report to Congress, August 2008, http://www.nuclear.gov/pdfFiles/NGNP_reporttoCongress.pdf