INL/CON-09-15887
PREPRINT

Integrating Safeguards and Security With Safety into Design

19th Annual EFCOG Safety Analysis Workshop

Robert S. Bean
John W. Hockert
David J. Hebditch

May 2009

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

Integrating Safeguards and Security with Safety into Design

Robert S. Bean
John W. Hockert
David J. Hebditch
Idaho National Laboratory (INL)
2525 N. Fremont Ave., Idaho Falls, ID 83415
(208) 526-7072 / (208) 526-6239 (FAX)

Abstract

There is a need to minimize security risks, proliferation hazards, and safety risks in the design of new nuclear facilities in a global environment of nuclear power expansion. In 2008, the U.S. Department of Energy (DOE) National Nuclear Security Administration (NNSA) launched the Next Generation Safeguards Initiative (NGSI), inter alia, to revitalize the technical base for safeguards in the United States and develop advanced safeguards concepts for the future. As part of NGSI, a team of representatives from four U.S. national laboratories and a U.S. university developed a proposed Safeguards-by-Design (SBD) process to ensure the timely, efficient, and cost effective implementation of international and domestic safeguards requirements with safety and other objectives into the overall design process for a nuclear facility. The proposed approach represents a graded, iterative process for accomplishing these goals through inclusion of appropriate design activities throughout all phases of the project plan. It was developed by using the DOE regulatory environment as a starting point. The relevant actions, deliverables, project interfaces, and organizational decision points necessary to incorporate both domestic and international safeguards were identified for a DOE project. The multi-laboratory team then produced a generic SBD process that could be employed for commercial projects within the U.S. or internationally for design of new facilities. Several tools for integrating safeguards, safety, and security into design are discussed herein. SBD appears complementary to the Safety and Security Interface Technology Initiative undertaken by the Energy Facility Contractor Group (EFCOG) in 2006 with input from NNSA, Defense Nuclear Security NA-70. That initiative focused on standardized upgrades to enable existing DOE facilities to meet more stringent standards. A collaborative approach among key stakeholders is suggested.

Introduction

The application of a process to enhance the integration of international safeguards and domestic safeguards with safety into the design of new commercial nuclear facilities has the potential to reduce the overall costs and the cost and schedule risks associated with meeting facility requirements. It also has the potential to reduce proliferation risks as the use of nuclear energy expands worldwide. This effort is a component of the U.S. Department of Energy's (DOE), Next Generation Safeguards Initiative (NGSI) and is jointly sponsored by the National Nuclear Security Administration (NNSA), Office of Nonproliferation and International Security (NA-24)

and the Office of Nuclear Energy.[1] To this end, DOE sponsored a multi-laboratory team in Fiscal Year 2008 to define a proposed process, known as Safeguards-by-Design (SBD), for accomplishing this objective, and to determine how it could be incorporated into existing facility design and construction processes.

While international, i.e. IAEA (International Atomic Energy Agency), safeguards cover the issue of nuclear material diversion by a State, activities by the State, i.e. domestic safeguards for nuclear material control and accountancy (MC&A) and physical security, defend against the threats of theft and sabotage by a non-host-State actor such as terrorists or agents of a rogue State. The nuclear material accountancy (MA), containment and surveillance (C&S), and design information verification (DIV) practiced as part of IAEA safeguards provide an independent verification of the accountancy reported by the State system of accounting for and control of nuclear material (SSAC), as well as the State actions for material control. In this paper, the phrase "safeguards and security" is equated with the combination of "international safeguards, other proliferation barriers and domestic safeguards."

In October 2008, the IAEA held a workshop focusing on its role in safeguards by design.[2] In April 2009, the IAEA held an International Symposium on Nuclear Security that included as an agenda item the 3S (safeguards, safety, and security) initiative.[3] During discussions in these two fora, it became clear that safeguards, safety, and security roles and definitions differ between the IAEA and the State level regulatory systems in different countries, and that the Agency has defined the components of 3S in the following ways. IAEA nuclear "safeguards" is the means applied to verify a State's compliance with its IAEA safeguards agreement on all nuclear material in all its peaceful nuclear activities and to verify that such material is not diverted to nuclear weapons or other nuclear explosive devices.[a] Nuclear "safety" is the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards. It concerns the protection of people and the environment against radiation risks, and the safety of facilities and activities that give rise to radiation risks. Nuclear "security" is the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear or other radioactive substances or their associated facilities and includes "physical protection."

The authors emphasize that the Safeguards-by-Design (SBD) process should integrate international safeguards and other proliferation barriers with domestic MC&A, physical security, and safety objectives; the proposed SBD process is not limited to a narrow definition of safeguards. It could ultimately help form the basis for a new international norm for integrating international safeguards into facility design. The results of this effort, including detailed requirements definition, SBD process flowcharts, and status of assessment methodologies are given in the report, INL/EXT-14777, *Institutionalizing Safeguards-by-Design: High-level*

[a] As a signatory to the "Treaty on the Non-Proliferation of Nuclear Weapons" (NPT), INFCIRC 140, April 1970, a non-nuclear-weapons State (NNWS) in respect to Article III: "…undertakes to accept safeguards, as set forth in an agreement to be negotiated and concluded with the International Atomic Energy Agency…" Details of this obligation are contained in "The Structure and Content of Agreements between The Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons," INFCIRC/153(Corrected), June 1972, which provides the basis for these negotiations for the implementation of a comprehensive safeguards agreement.

Framework and an associated paper.[4,5]

This paper describes the generic activities needed for the proposed SBD process in each phase of design. It builds on the guidance provided in DOE Guide 413.3-3, *Safeguards and Security for Program and Project Management*,[6] but then structures the SBD process to a more generalized phasing of design. It summarizes these results with particular focus on those aspects of SBD that support the integration of safeguards, safety and security considered broadly. Wider aspects of SBD and supporting methodologies for improving the safeguardability of nuclear facilities have been examined.[7] This paper covers specific tools for this purpose. Future work activities are discussed and conclusions drawn.

SBD Process

Project Management and Design Phases

Within the context of the DOE Order 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, there are five phases of facility design with the last one finishing during construction, see Figure 1.[8] The planning phase consists of activities, including pre-conceptual design, supporting Critical Decision 0 (CD-0), *Approval of Mission Need.* CD-1, *Approval of Alternative Selection and Cost Range* forms the completion of conceptual design. The preliminary design phase consists of the activities supporting CD-2, *Approval of Performance Baseline* (preliminary design), and CD-3, *Approval of Start of Construction* (completion of final design). The construction phase consists of the remainder of the project. Initially, as an example study, the proposed SBD process[4,5] was tailored to the DOE oversight environment and made extensive use of the DOE design and construction process, defined in DOE O 413.3A.

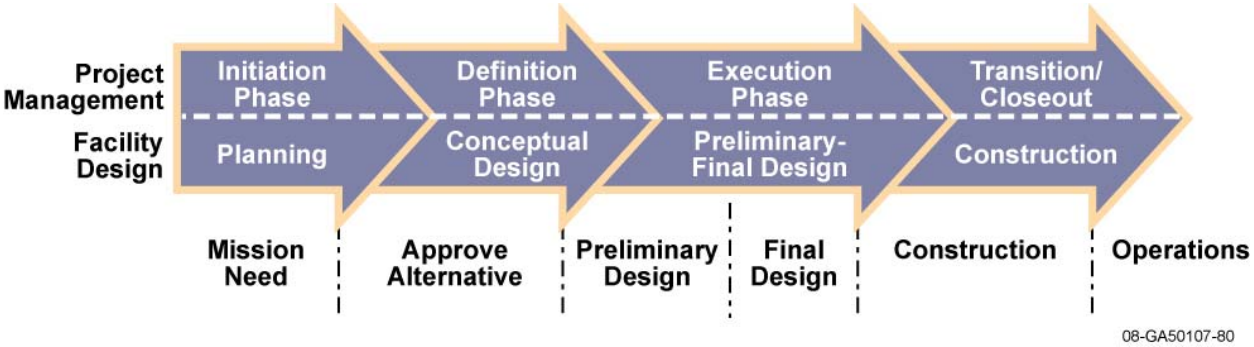

Figure 1. DOE phases of project management and design processes.[8]

A recent NNSA objective under the NGSI was to form a broader proposed SBD process that can be employed both within the U.S. licensed nuclear industry and internationally. This later SBD process needs to be sufficiently generic to adapt to the project management approaches and regulatory structures used in the commercial nuclear industry in the United States and other

nations. Since the signing of the U.S.-IAEA Safeguards Agreement in 1977, over 200 facilities licensed by the NRC have been placed on the list of U.S. facilities eligible for IAEA safeguards reporting and inspections. Unlike a non-nuclear weapons state (NNWS), the US is not obligated to have its civilian nuclear facilities under IAEA Safeguards as an NPT signatory. During NPT negotiations, NNWS expressed concerns that this would put them at a disadvantage to weapons states. To allay these concerns, the US made a voluntary offer to accept IAEA safeguards on their peaceful nuclear activities. This offer was codified in INFIRC/288 - The Text of the Agreement of 18 November 1977 Between the United States of America and the Agency for the Application of Safeguards in the United States of America. Several facilities selected by the IAEA as part of this offer have submitted accounting data to the IAEA and at least one has undergone IAEA inspection in the past. When the U.S. Additional Protocol to the NPT entered into force in January 2009, all U.S. eligible facilities, i.e. those without activities associated with direct national security significance, became subject to strengthened reporting requirements and expanded IAEA access rights. This includes all new U.S. commercial nuclear facilities that may be designed, constructed and operated. In general, the design and construction process for complex nuclear facilities can be divided into three main phases: planning (including conceptual design), design (preliminary and final design), and construction. This is the basis for the following description of the proposed generic SBD process.

Outline of SBD Process

The proposed SBD process includes development of an overall design strategy for international safeguards and other proliferation barriers, with domestic MC&A and physical security. This documents the design approaches that the project proposes to meet the physical security requirements from directives, the performance requirements from performance analyses commensurate with the maturity of the design and complexity of the facility, the domestic safeguards significance of the nuclear material housed at the facility, and the international safeguards needs as required by DOE and derived from IAEA criteria provided in the Safeguards Manual.[9] Another analysis identifies the design features and associated performance requirements needed to meet intrinsic and extrinsic proliferation risk reduction requirements.

Within each phase, the SBD team employs design information from the overall facility project design to perform iterative design activities to establish specialized safeguards and security measures. As in all design activities, these cover requirements definition, design, assessment of design effectiveness, re-iteration of design if needed, and exit to project design review when appropriate with subsequent repetition if needed. Collaboration with other specialist design team members, including safety, is required to address design interfaces and interactions. As discussed below, this collaboration is accomplished on the small scale through interdisciplinary reviews and at the overall project level via the systems engineering process. Design definition increases in each design phase while the overall pattern is repeated for comment resolution as necessary. There are iterations of this safeguards and security design method in each of the three design phases: planning, design, and construction. The generic SBD process accomplishes its goals through inclusion of appropriate design activities in the project plan and their execution according to modern project and systems engineering practices.

Main Generic SBD Activities during the Planning Phase[b]

The main activities of the proposed SBD process during the planning phase are:

a) Participation of safeguards subject matter expert(s) in concept development.
b) Identification of facility risk-based safeguards and security categorization (such as those used in Section 5 of INFCIRC 225[10] for physical protection) and the associated requirements as early in concept development as practicable.
c) Identification of applicable safeguards requirements, using the graded approach based on safeguards categorization. These safeguards requirements, e.g. for physical protection, are separated into prescriptive requirements (e.g., security areas, physical barriers, intrusion detection) and performance requirements (e.g., ability to contain adversaries with design basis threat capabilities, and capability to detect the loss of significant quantity of special nuclear material). For facilities subject to IAEA safeguards, the applicable international safeguards requirements should also be identified and addressed.
d) Establishment of the level of formality of the SBD process using the graded approach based on safeguards categorization and the applicability of standard safeguards design approaches (e.g., the extent of facility standardization).
e) Incorporation of the prescriptive requirements into the design concept using the project systems engineering process.[11]
f) Development of conceptual strategies for meeting safeguards performance requirements including: (1) use of "off-the-shelf" safeguards measures, (2) research and development needed to enhance existing measures and/or develop new measures, and (3) design features to enhance protectability and safeguardability (intrinsic measures). This includes development of unclassified design requirements to implement the conceptual strategies and incorporation of these requirements into the design concept using the project systems engineering process.
g) Completion of analyses demonstrating, with the appropriate level of assurance, that the conceptual strategies will meet the safeguards performance requirements. (At this stage of the project, these analyses should make conservative assumptions related to uncertainties in the capabilities of safeguards measures and overall design.)
h) Identification of a “safeguards envelope” (the set of design features and associated requirements relied on for meeting safeguards prescriptive and performance requirements) at an appropriate level of detail with the imposition of limited configuration management.
i) Preliminary assessment of project risk associated with conceptual strategies for meeting safeguards performance requirements, including risk mitigation strategies (e.g., research and development, design changes).
j) Documentation of the safeguards categorization, applicable requirements, conceptual strategies developed for meeting performance requirements, safeguards envelope, and project risk assessment. These documents should be formally approved by the project owner and cognizant regulators, as applicable, as part of the authorization to proceed to the next phase.

[b] Here “safeguards” refers to domestic safeguards and/or international safeguards.

Main Generic SBD Activities during the Design Phase[c]

The main activities of the proposed SBD process during the design phase are:

a) Continued participation of safeguards subject matter experts in design development, including the expectation of leadership in safeguards design and review of all changes affecting the safeguards envelope.
b) Validation of safeguards categorization and applicable requirements as the design matures.
c) Refinement of strategies for meeting safeguards performance requirements as the design matures and modification of associated design requirements, including the safeguards envelope, based on refined strategies and maturing design. Like other aspects of the design, the safeguards measures are subject to increasingly stringent configuration management as the design matures.
d) Refinement of the analyses demonstrating that the safeguards strategies will meet the safeguards performance requirements, reflecting the maturing design, the reduction of uncertainties associated with the capabilities of safeguards measures and the design details, and the corresponding ability to use more sophisticated analytical approaches.
e) Refined assessment of project risk associated with strategies for meeting safeguards performance requirements, including refinement of risk mitigation strategies based on maturing design and results of research and development activities. Implementation of risk management strategies as required.
f) Continued systems engineering and design activities to meet prescriptive safeguards requirements and design requirements associated with strategies for meeting safeguards performance requirements.
g) For facilities potentially subject to IAEA safeguards, activities during this phase include collaboration with the IAEA regarding information to be provided in the Design Information Questionnaire, as early as practicable, and the negotiation of the Facility Attachment.
h) Refinement, development, and re-approval of the safeguards design and analysis documents formally approved by the project owner and cognizant regulators, as applicable, as part of the authorization to proceed to the next phase.

Main Generic SBD Activities during the Construction Phase[d]

The main activities of the proposed SBD process during the construction phase are:

a) Continued participation of safeguards subject matter experts in review of field and design changes affecting the safeguards envelope.
b) Refinement of the analyses demonstrating that the safeguards strategies will meet the safeguards performance requirements. The refinement of these analyses reflects design changes in the field, the demonstrated capabilities of safeguards measures, and the detailed as-built configuration.
c) Initial and continuing systems engineering and quality assurance validation activities, including performance validation, to verify that the as-built design meets safeguards

[c] Here "safeguards" refers to domestic safeguards and/or international safeguards.
[d] Here "safeguards" refers to domestic safeguards and/or international safeguards.

requirements, as construction proceeds. This also includes safeguards acceptance reviews and validation at the conclusion of construction prior to turnover of the facility and/or process for operation.

d) Development of plans, policies, and procedures to implement strategies for meeting safeguards performance requirements in operation, including minor strategy modifications to address operational constraints.
e) For facilities subject to IAEA safeguards, IAEA design information verification activities begin and the delivery and installation of IAEA safeguards equipment is completed during this phase. At the completion of construction, all equipment necessary for implementation of IAEA safeguards is to be installed, tested, and accepted.
f) Continued refinement and development of safeguards analysis documents, including by the end of construction (1) the results of safeguards acceptance reviews and validation and (2) the commitment documents (e.g., security plans, MC&A plans) required for safeguards approval of facility operation.

Key Features and Benefits of the SBD Process

After integrating the SBD process, by means of flowcharts,[4,5] with that for DOE design and construction management, etc.,[6,8,11,12] the multi-laboratory team extracted the fundamentals. The team determined that the principal features of the proposed generic SBD process are:

a) Early involvement of the SBD team in the design effort.
b) Early identification of international safeguards, MC&A, and physical security requirements.
c) Early formulation of intrinsic features that will enhance the protectability and proliferation resistance (including safeguardability) of the design.
d) Closer integration of international safeguards, MC&A, and physical security with project design.
e) A clear and simple plan for ensuring effective interaction between international safeguards, MC&A, physical security, and the facility design process, which identifies the required activities and timeline and provides detail and analyses in each phase of design.
f) Specific requirements for owner and/or stakeholder approval of design approaches and associated risks at key decision points.
g) Sufficient flexibility to incorporate all regulatory requirements into the design of nuclear facilities.

By encouraging the design and development of safeguards and security (i.e. international safeguards, other proliferation barriers and domestic safeguards) measures early in the design, the proposed SBD process reveals areas where there are potential conflicts between safety, and safeguards and/or security early in the project planning and design process, when they can be resolved at lower cost and schedule impact. Similarly the early and open communication of safeguards and/or security requirements will help the safety subject matter experts identify areas of potential conflict earlier in the project planning and design process. The incentives in DOE-STD-1189-2008, *Integration of Safety into the Design Process,*[12] for developing safety design features and considering safety requirements earlier in the design process also support early

identification of challenges to integrating safety, as one entity, with safeguards and/or security as the other. Early identification of areas of potential conflict also makes it possible to formulate and gain approval of equivalent alternative approaches with much reduced risk in project cost and schedule.

The use of the systems engineering process for the incorporation of safety requirements together with safeguards and security requirements into the design will aid in ensuring that the areas of potential conflict will be identified and resolved. The systems engineering process[11] provides a structured approach for identification of trade-offs in areas of potential conflict between safety, and safeguards and security. However, it is important to note that, in some areas, such as radiological sabotage protection, it may be possible to find complementary design approaches that enhance both safety, and safeguards and security characteristics.

Thus, the SBD process, in combination with the safety integration process mandated by DOE-STD-1189-2008 provides increased assurance that integration challenges will be identified early in the design process when conflicts can be resolved or equivalent alternative approaches can be developed with lower cost and schedule impact. Detailed approaches for the resolution of challenges for the integration of safety, with safeguards and security, are beyond the scope of high level processes, like the proposed SBD process and the DOE-STD-1189-2008 safety integration process. The most that such processes can achieve is providing a structured approach assuring that 1) challenges for the integration of safety, with safeguards and security, will be identified early in the design process, 2) requirements in the areas of safety, and safeguards and security, are clearly identified and communicated to and within the project, and 3) design information about safety measures, and safeguards and security measures, is clearly communicated within the project so that areas of interaction can be identified. Such processes also provide the project management with identification of conflict between competing disciplines and requirements, thereby enabling a healthy decision process for conflict resolution.

Potential benefits of application of the SBD process include the following:[3,4,5,7]

a) Lowering nuclear security risks and proliferation hazards, and enhancing the safety of new nuclear facilities in an economical way, while raising operational efficiency.
b) Determining, using lifecycle cost analysis, the trade off between intrinsic (mainly capital cost) and extrinsic (mainly operational cost) features.
c) Helping stakeholders including the IAEA and the owner and/or operator.
d) Providing an SBD process framework that can be readily integrated with current nuclear facility design processes, including the possibility of demonstrating its feasibility and usefulness in pilot tests on current design projects.
e) Increasing the effectiveness and efficiency of the design process for international safeguards, physical security and MC&A, and for safety.
f) Improving project risk management and reducing project cost and schedule risks.
g) Supporting almost all regulatory, project management, and engineering environments, across a wide range of nuclear facilities.
h) Supporting recent U.S. NRC policy for advanced nuclear energy systems that requires concurrent consideration of safety and security requirements while designing a facility, with the goal that safety and security will require fewer human actions. This policy also

requires early consideration of international safeguards.[13]

Tools for Integrating Safeguards, Safety, and Security into Design

Although specific methodologies for integration of safeguards, safety, and security (together equated with international safeguards, other proliferation barriers, safety, domestic physical security, and MC&A) are not integral parts of either the proposed SBD process or the DOE-STD-1189-2008 safety integration process, there are some design tools that are enable these processes and can assist designers in overcoming these integration challenges. Section 7.8 of DOE-STD-1189-2008 points out two areas where safety, and safeguards and security integration is particularly important.

The first is the design of structures, where the integration challenges generally relate to life safety issues, such as the effect of barriers and access control measures on the length of exit paths and number of emergency exits. There may also be significant synergies in the structural area where the same structural design may provide both a substantial physical protection barrier and protection against natural phenomena and impact loads, e.g., aircraft crash.

The second area where integration is particularly important is consideration of the hazards posed by security measures. These may be life safety hazards or may be significant enough to affect nuclear safety (e.g., accidental firearm discharge). Obviously, the safety analysts must be sufficiently aware of the safeguards and security measures employed in the design to consider the related hazards in the hazard and accident analyses. This is an area where the SBD process mandate to define and develop safeguards and security measures early in the design supports the DOE-STD-1189-2008 process mandate for thorough hazards and accident analysis early in the design process.

A third area where there may be significant synergy between safety, and safeguards and security is in process design for accurate MC&A measurements. Such measurements may also support controls for nuclear criticality safety. Even if the same measurements are not used for both purposes, a process design that supports accurate MC&A measurements will also support accurate measurements for nuclear criticality safety purposes.

There are several types of tools that can be employed to facilitate safeguards, safety, and security integration. The first is the development of a library (or toolbox) of safeguards and security measures that have been evaluated for both their safeguards and security effectiveness and for their associated hazards. This approach was detailed in the *Topical Report on Security and Safety Integration*[14] (TROSSI) that the Energy Facilities Contractors Group (EFCOG) prepared as a part of the EFCOG Safety and Security Interface Technology Initiative. The main advantage of this approach is that individual projects can employ standard safeguards and security measures and adopt the already established security effectiveness and hazard analysis results. If the oversight organizations have pre-approved the standardized safeguards and security measures and security effectiveness and hazard analysis results, then this approach also helps reduce project regulatory risk. The approach obviously works best in situations where the security design basis threat is similar from facility to facility so that the MC&A and physical security

effectiveness can be meaningfully determined.[e] It also is most useful for facility types and designs and for protection strategies which are sufficiently similar that the designer can select from a relatively small range of safeguards and security design measures to create a design that provides the requisite protection. These factors make the toolbox approach especially useful for projects like the upgrades of DOE facility safeguards and security to a more severe design basis threat, for which the *Topical Report on Security and Safety Integration* was intended.[14] The new design basis threat was the same, or at least similar, for all the facility upgrades and the facilities to be upgraded all employed the safeguards and security protection strategy mandated by the DOE orders. In situations where the design basis threat varies significantly between facilities or projects and protection strategies vary from one country to another, the toolbox approach is likely to be less valuable. In such situations there may also be security restrictions that prevent the sharing of information about safeguards and security design measures and their vulnerabilities. The recently established World Institute for Nuclear Security (WINS) has the objectives to foster the establishment of an international physical security culture and provide an international forum for the sharing of security relevant information.

A second, related tool can be developed by sharing approved security effectiveness and hazard and accident analysis results among projects within a single country. This approach may be useful, particularly if a large number of similar facilities (e.g., nuclear power reactors) are being designed and built. This second approach is simpler in that it requires only the collection and documentation of evaluations and analyses that have already been accomplished and approved without the additional effort of selecting and modeling candidate safeguards and security measures to prequalify them for the library.

A third type of tool would be a set (or toolbox) of approved approaches, or methodologies, for analyzing the effectiveness of MC&A and physical security measures and for hazard and accident analysis. The DOE has a set of tools that they have judged acceptable in both areas, although both safeguards and security effectiveness analysis and hazard and accident analysis involve modeling of quite complex phenomena with significant uncertainties. As a result, methods that are acceptable to the regulatory and/or oversight organizations in one nation state might not be acceptable to those in another. The IAEA has provided international guidance on much of the modeling required for hazard and accident analysis.[15-21] However, there is much less guidance for physical security effectiveness modeling. This may be because the physical security element received less attention prior to the terrorist attacks on September 11, 2001. Also, the complexity of modeling physical security effectiveness is significantly greater than hazard or accident modeling. The malevolent intelligence of the adversary causes greater difficulty in modeling physical security effectiveness. This enables targeting of the most vulnerable safeguards and security measures and actions to disable specific safeguards and security measures. It is difficult to model the complex interaction between perceived safeguards and security effectiveness and the targeting decisions made by the adversary (i.e., deterrence). Still, standardized modeling approaches have the potential to provide figures of merit that are useful in comparing the effectiveness of different sets of safeguards and security measures.

There is less consensus regarding the development of quantitative analysis measures for

[e] The effectiveness of a specific MC&A or physical security measure can vary dramatically depending upon the design basis threat.

evaluating and comparing the proliferation resistance of facility process designs and safeguards and security measures, e.g. PR-PP (proliferation resistance and physical protection) as developed under the Generation IV International Forum, and INPRO Manual – Proliferation Resistance as developed by the IAEA.[22-24] Although the main focus of such tools is proliferation resistance and physical security measures, the tools would be useful in comparing alternative measures identified to resolve potential conflicts between safety with physical security measures. An approved set of evaluation tools would also facilitate the sharing of approved security effectiveness and hazard and accident analyses results among projects.

Future Work Activities

The multi-laboratory team has formulated a generic SBD process[3,4,5,7] which supports the potential formation of an international norm for the nuclear industry. The focus of near term future activities is to assess the costs, benefits, and practicality of this proposed approach with the objective of further refining it, including stakeholder review, prior to potential implementation. Supporting work is progressing with the development of general guidelines, facility specific guidelines, best practices, increased definition of requirements, and criteria for acceptance. Specific features for early development include the definition and scope of proposed safeguards effectiveness reports and the application of lifecycle cost analysis to the optimization of design with regard to trade-offs between design features and more labor intensive protection measures. The multi-laboratory team intends to examine the lessons learned from current projects, implemented without SBD, to determine whether they would have benefited significantly from an SBD approach and to identify additional good practices for possible incorporation into the SBD approach or design guidance. If supported by these analyses, the follow-on to this effort would be the development of an institutionalization strategy for the SBD process, taking advantage of the applicable lessons learned from the institutionalization of the safety integration process. The EFCOG Safety Analysis Working Group and the Security Working Group could provide valuable insights regarding the costs, benefits, and practicality of the SBD approach proposed for DOE projects and the feasibility of candidate institutionalization strategies. The experience of the EFCOG Safety Analysis and Security Working Groups in the development and institutionalization of the DOE process for integration of safety with design could also make a significant contribution to these efforts

These U.S. efforts support the creation of a possible international norm for safeguards by design and complement an international interest in the development of an SBD process in the international safeguards context, as exemplified by recent IAEA fora.[2,3] Industry use of the proposed SBD process may need industry initiatives based on firm evidence of value, such as pilot testing or demonstrations, or the introduction of formal requirements, e.g. regulations. These do not yet exist given the early stage of development. Tests or other activities, that illustrate the benefits of applying the SBD process, would be of particular value.

Conclusions

The multi-laboratory team draws the following conclusions:

1. The paper presents the main goals for a proposed generic Safeguards-by-Design (SBD) process based on the generalized design phases of planning, design, and construction, which enhances integration of safeguards, safety, and security in the acquisition of new nuclear facilities. The generic SBD process accomplishes its goals through inclusion of appropriate design activities in the project plan, and their execution under the governing project management and systems engineering systems.

2. The emphasis of the proposed SBD process is on the early design phases, definition of the design requirements, safeguards design assessment, selection of major design options, intrinsic safeguards features, life-cycle cost and schedule risk management, and design and risk communication with major stakeholders.

3. The generic SBD process was drawn from a proposed detailed SBD process prepared for the DOE regulatory environment, including international safeguards, that is ready for wider stakeholder review and pilot testing.

4. The generic SBD process can currently be used on a test basis, is applicable to a wide range of nuclear facilities and regulatory environments, and is supportive of international SBD work initiated recently by the IAEA and also the longer term 3S (safeguards, safety, and security) integration being examined by the IAEA.

5. Several design tools provide methodologies which support the proposed SBD process and the DOE-STD-1189-2008 safety integration process and can be employed to facilitate safeguards, safety, and security integration. Continuing development of a library (or toolbox) of measures that have been evaluated for safeguards and security effectiveness and/or approved approaches for analyzing the effectiveness of safeguards and security measures and for hazard and accident analysis is encouraged.

6. The experience of the Safety Analysis Working Group and Security Working Group of the Energy Facility Contractors Group (EFCOG) in development of the "Topical Report on Security and Safety Integration" is relevant to analysis of the costs, benefits, and practicality of the proposed SBD approach and the feasibility of candidate SBD institutionalization and deployment strategies.

Acknowledgments

The authors gratefully acknowledge support under the U.S. DOE's Next Generation Safeguards Initiative (NGSI) and permission to publish from the DOE.

References

1. DOE, National Nuclear Security Administration: Nuclear Nonproliferation, http://nnsa.energy.gov/nuclear_nonproliferation/nuclear_safeguards.htm , NNSA Next Generation Safeguards Initiative, 2008.
2. IAEA, Facility Design and Plant Operation Features that Facilitate Implementation of IAEA Safeguards, SGCP-CCA, Report STR-360, February 2009.
3. R.S. Bean, T.A. Bjornard and D.J. Hebditch, Safeguards-by-Design: An Element of 3S Integration, International Symposium on Nuclear Safety, Paper IAEA-CN-166/067, 10 pages, Vienna, Austria, April, 2009.
4. T.A. Bjornard, J.E. Alexander et al., Institutionalizing Safeguards-by-Design: High Level Framework, Idaho National Laboratory, Report INL/EXT-14777, Volumes 1 and 2, 212 pages, 2008.
5. T.A. Bjornard, R.S. Bean et al., Safeguards-by-Design: Early Integration of Physical Protection and Safeguardability into Design of Nuclear Facilities, Paper #9518, 10 pages, submitted to Global 2009 International Conference, Paris, Sept 6-11, 2009.
6. DOE, Guide 413.3-3, Safeguards and Security for Program and Project Management, U.S. Department of Energy, November 15, 2007.
7. T. Bjornard, R. Bari, et al., Improving the Safeguardability of Nuclear Facilities, Paper invited to Special Summer Issue, Journal of Nuclear Materials Management, INMM, Deerfield, IL, USA, 17 pages, 2009.
8. DOE, Order 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, U.S. Department of Energy, July 28, 2006.
9. IAEA, Department of Safeguards: Safeguards Manual – Parts SMI and SMC, Safeguards Criteria and Annexes, International Atomic Energy Agency, Vienna, Austria, January, 2004.
10. IAEA, INFCIRC/225/Rev. 4, The Physical Protection of Nuclear Material and Nuclear Facilities, International Atomic Energy Agency, Vienna, Austria, June, 1999.
11. DOE, Guide 413.3-1, *Managing Design and Construction Using Systems Engineering for Use with DOE O 413.3A,* U.S. Department of Energy, September 23, 2008.
12. DOE, Standard STD-1189-2008, *Integration of Safety into the Design Process,* U.S. Department of Energy, March, 2008.
13. NRC, NRC Issues Advanced Reactor Design Policy, News No. 08-189, October 14, 2008.
14. EFCOG, Topical Report on Security and Safety Integration (TROSSI), Prepared for the: Safety and Security Interface Technology Initiative, Energy Facility Contractors Group, September 11, 2006.
15. IAEA, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plans (Level 1), 50-P-4, International Atomic Energy Agency, Austria, June, 1992.
16. IAEA, Generic Models for Use in Assessing the Impact of Discharges of Radioactive Substances to the Environment, Safety Reports Series, No.19, Vienna, Austria, June, 2001.
17. IAEA, Derivation of the Source Term and Analysis of the Radiological Consequences of Research Reactor Accidents, Safety Reports Series, No.53, Vienna, Austria, 2008.
18. IAEA, Use of Computational Fluid Dynamics Codes for Safety Analysis of Nuclear Reactor Systems, IAEA-TECDOC-1379, Vienna, Austria, November, 2003.
19. IAEA, Incorporation of Advanced Accident Analysis Methodology into Safety Analysis Reports, IAEA-TECDOC-1351, Vienna, Austria, May, 2003.
20. IAEA, Safety Analysis of Nuclear Power Plants during Low Power and Shutdown Conditions, IAEA-TECDOC-1042, Vienna, Austria, September, 1998.

21. IAEA, Safety Series No. 64, Safety Analysis Methodologies for Radioactive Waste Repositories in Shallow Ground, Vienna, Austria, May, 1984.
22. Generation IV International Forum, Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems, The PR-PP Evaluation Methodology Expert Group, GIF/PRPPWG/2006/005, Revision 5, pp. 65-69, November 30, 2006.
23. International Atomic Energy Agency, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual - Proliferation Resistance, Volume 5 of the Final Report of Phase 1 of the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO), 2007.
24. G. Pomeroy, R. Bari, et al., Approaches to Evaluation of Proliferation Resistance of Nuclear Energy Systems, 49th Annual Meeting of INMM, Nashville, TN, 8 pages, July 13-17, 2008.