INL/CON-09-15834
PREPRINT

Improving the Safeguardability of Nuclear Facilities

Institute of Nuclear Materials Management 50th Annual Meeting

T. Bjornard
R. Bari
D. Hebditch
P. Peterson
M. Schanfein

July 2009

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

Improving the Safeguardability of Nuclear Facilities

T. Bjornard[1], R. Bari[2], D. Hebditch[1], P. Peterson[3], M. Schanfein[1]
1. Idaho National Laboratory, Tel: 1-208-526-6328, Fax: 1-208-526-6239,
E-mail: Trond.Bjornard@inl.gov
2. Brookhaven National Laboratory, 3. University of California, Berkeley

Abstract – The application of a Safeguards-by-Design (SBD) process for new nuclear facilities has the potential to reduce security risks and proliferation hazards while improving the synergy of major design features and raising operational efficiency, in a world where significant expansion of nuclear energy use may occur. Correspondingly, the U.S. DOE's Next Generation Safeguards Initiative (NGSI) includes objectives to contribute to international efforts to develop SBD, and to apply SBD in the development of new U.S. nuclear infrastructure. Here, SBD is defined as a structured approach to ensure the timely, efficient and cost effective integration of international safeguards and other nonproliferation barriers with national material control and accountability, physical protection, and safety objectives into the overall design process for a nuclear facility, from initial planning through design, construction and operation. The SBD process, in its simplest form, may be applied usefully today within most national regulatory environments. Development of a mature approach to implementing SBD requires work in the areas of requirements definition, design processes, technology and methodology, and institutionalization. The U.S. efforts described in this paper are supportive of SBD work for international safeguards that has recently been initiated by the IAEA with the participation of many stakeholders including member States, the IAEA, nuclear technology suppliers, nuclear utilities, and the broader international nonproliferation community.

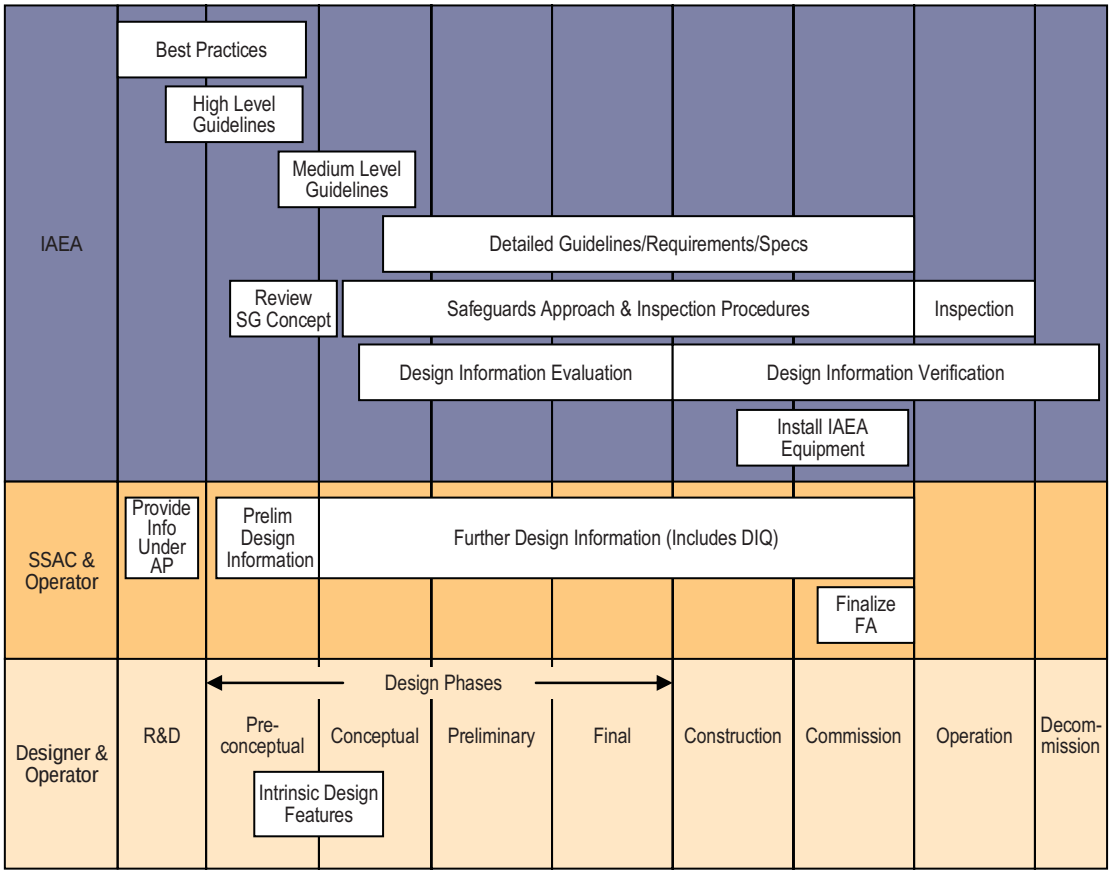
1. INTRODUCTION

The nuclear industry has made significant operational and design advances in recent decades, notably in the area of safety. These developments, triggered by the accidents of Three Mile Island and Chernobyl reactors, resulted in nuclear energy systems that operate with impressive safety and reliability performance and in designs for future reactor systems where safety is considered as an integral part of the design process. Industry has learned that it is cost effective, from the earliest conceptual stages, to design safety into the facility. Also, since the World Trade Center attacks of September 11, 2001, increases in physical security requirements at U.S. nuclear facilities have resulted in the need for costly security upgrades, underscoring the urgency of designing future facilities to be intrinsically more secure with decreased reliance on the action of protective forces.

A design approach to cost-effectively mitigate emerging security threats as new nuclear energy systems are designed and deployed will have significant impact in a global environment of nuclear energy expansion. Proliferation resistance is defined by the IAEA as "that characteristic of a nuclear energy system that impedes the diversion or undeclared production of nuclear material or misuse of technology by the state seeking to acquire nuclear weapons or other nuclear explosive devices". Effective IAEA safeguards are a key element contributing to proliferation resistance, in addition to other intrinsic (design) and extrinsic (institutional) features, here described as 'other proliferation barriers'. Safeguardability, in turn, refers to the extent to which the design of the facility readily accommodates, and facilitates, effective and cost-efficient safeguards for the facility. The proposed Safeguards-by-Design (SBD) process, described in this paper, is an approach which integrates safeguards with physical security and safety during design to improve the safeguardability of nuclear facilities.

2. IAEA LED INTERNATIONAL INITIATIVE TO DEVELOP SAFEGUARDS-BY-DESIGN

The IAEA launched its exploration of the concept of Safeguards-by-Design by hosting an international workshop entitled "Facility Design and Plant Operation Features that Facilitate the Implementation of IAEA Safeguards" in autumn 2008 at its headquarters in Vienna, Austria. The workshop was well attended by participants from Member States, the European Commission, nuclear industry, and the IAEA [1]. IAEA has clear responsibility to apply international safeguards, through treaties and other agreements employing monitoring and verification, while the Agency's role in safety and security is only advisory. Recognizing this distinction, the IAEA workshop participants focused on IAEA safeguards, in particular, when they defined a proposed IAEA SBD process as "an approach wherein safeguards are fully integrated into the design process of a nuclear facility - from initial planning through design, construction, operation, and decommissioning." The IAEA defines safeguards as "the means applied to verify a State's compliance with its undertaking to accept an 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."



SSAC = State system of accounting for and control of nuclear material; AP = Additional protocol; SG = Safeguards; DIQ = Design information questionnaire; FA = Facility attachment.

Fig. 1. Activities Timeline for IAEA Proposed Safeguards-by-Design Process [1]

SBD is expected to facilitate reaching objectives, such as: a. enhancing safeguardability in new nuclear facilities; b. reducing the time and cost for the inspectors' physical presence at facilities; c. incorporating authentication and use of process monitoring data into the safeguarding of selected nuclear facilities; d.

facilitating joint-use of equipment and instrumentation between the operator and the IAEA; and e. eliminating retrofit of instrumentation needed by IAEA and increasing flexibility for future equipment installation.

The workshop participants strongly endorsed the integration of safeguards into the design of new facilities earlier than is presently done. A timeline of actors and activities was prepared to show the necessary interactions and cooperation, see Fig.1. Further workshop recommendations include: revising the IAEA Safeguards Manual to take account of the SBD initiative, providing IAEA safeguards documentation to facility designers immediately, creating several expert working groups tasked with defining the SBD process and creating an implementation strategy, developing new design guidelines organized by facility type that can be published as part of the IAEA Nuclear Energy Series, and providing general SBD process timelines for nuclear facilities in various stages, e.g. operational, evolutionary, and new design. Various beneficial design characteristics were identified which included:

- Clear safeguards vision and guidelines
- Availability of safeguards guidelines to enable compliant and/or optimized plant to be built with minimal impact on the operator and designer/constructor
- Early integration of safeguards in the design phase to minimize impact on production, and enable easy maintenance, and unattended operation
- Detailed knowledge by operators of safeguards systems to be applied to future facilities
- Improved integration of safeguards with safety and security
- Timely advice of IAEA needs to avoid retrofitting
- Verification of signal authenticity for joint-use equipment during design information verification
- Effective stakeholder engagement in design phase minimizing changes during construction

Consistent with the proposals of the workshop, the following iterative process between the IAEA, SSAC, and facility operator is suggested in this paper for implementation of SBD. Following receipt of early design information, the Agency will propose material balance areas (MBA) based on the facility design, nuclear material (NM) flows, NM composition, and the desire to meet both IAEA quantity and timeliness goals. In each MBA, both the operator and the IAEA (independently) must be able to close the material balance and evaluate any difference between the beginning and ending inventory.

The IAEA will then propose a safeguards approach that includes both key measurement and strategic points in the facility as well as the measurement/monitoring equipment to accomplish the approach. This negotiation between the three parties to finalize this approach can result in any combination of the measurement/monitoring techniques including:

a) Fully independent IAEA equipment
b) Joint Use Equipment whose data is shared between the facility operator and the IAEA
c) Joint Use Equipment whose data is not shared and whose data set could be all collected data or some subset dependent on IAEA needs

In all cases this equipment is fully integrated into the project management system to assure all cost, schedule, and performance requirements are met including provisions for addressing authentication needs of the IAEA. Clearly all parties need to negotiate agreement to final requirements and this includes learning of and assessing potential alternate approaches that still allow independent IAEA verification but also address facility operational needs.

3. SAFEGUARDS-BY-DESIGN WITHIN A NATIONAL REGULATORY STRUCTURE

3.1 State Level support to IAEA

While international (IAEA) safeguards focus on the issue of nuclear material diversion by a State, requirements prescribed by a State 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. For this reason it is vital to the IAEA SBD process that State requirements for MC&A and security also be dealt with early in the design process. Because of the close connection between State level MC&A and physical security, and the numerous interconnections between security and safety, it becomes evident that in order to properly support an SBD process for IAEA safeguards it is necessary to include MC&A, physical security and safety in formulating and executing the overall SBD process. In other words, in order for SBD to succeed, the international safeguards effort for MA, C&S, and DIV must be fully supported at the level of domestic safeguards and security.

3.2 Next Generation Safeguards Initiative supporting Safeguards-by-Design

Support of the Safeguards-by-Design (SBD) process is a fundamental part of the Next Generation Safeguards Initiative (NGSI) prepared by the U.S. DOE National Nuclear Security Administration (NNSA). This U.S. initiative is supportive of international efforts to develop SBD to ensure the timely, efficient, and cost-effective implementation of international safeguards, while concurrently ensuring the proper integration of national MC&A, physical protection, and safety features into future nuclear energy infrastructure. A major objective is to demonstrate and institutionalize SBD [2].

The SBD approach requires the identification and integration of international safeguards requirements (in addition to national MC&A, physical protection, and safety requirements) into the design of a nuclear facility at the earliest stages of conceptual design. These “requirements” are high level, flexible in some aspects to enable best safeguards performance and negotiated between the Agency and the State. Once and whatever agreed, they become design requirements. Synergy in design of structures, systems and components (SSC) provides intrinsic barriers, for example a reactor containment vessel or underground placement may help provide security against some malevolent actions as well as enhancing safety. Effective implementation of SBD avoids potentially expensive and time-consuming retrofitting of a facility during and after startup and operation. SBD also focuses on the idea that efficient design for safeguards will make it easier for an operator and State to perform satisfactory nuclear MC&A and process control, which can reap performance and cost advantages for the facility operator. Hence, good safeguards design can mean good business practice, where safeguards are designed with the goal to be integrated with facility process control rather than being added later as another layer. In this way, safeguards may work in the background as part of a normal process and have minimal impact on facility throughput.

The NGSI also declares the importance of developing guidelines, requirements, and best practices. Institutionalizing of SBD will depend on the development of universally agreed requirements, clear guidelines, and a catalog of best practices. Guidelines and requirements would include recommendations for established safeguards systems as well as techniques and methods for particular applications or facilities.

Accordingly, the need exists to develop a simple, formalized, and integrated approach, and introduce this into nuclear facility design and construction management. Institutionalizing Safeguards-by-Design (ISBD) is the implementation of a structured approach by which international safeguards objectives, and national material control and accountability (MC&A), physical protection and safety objectives can be 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. Application of SBD in the facility design and construction effort is intended to provide: early identification of safeguards requirements, inclusion of intrinsic features, optimization of facility alternatives, reduced impact to operation, minimization of life-cycle cost, and minimization of equipment retrofit [3]. International efforts to develop SBD as a standard approach in nuclear system design would enable the efficient growth of nuclear power to occur while reducing nuclear proliferation and security risks.

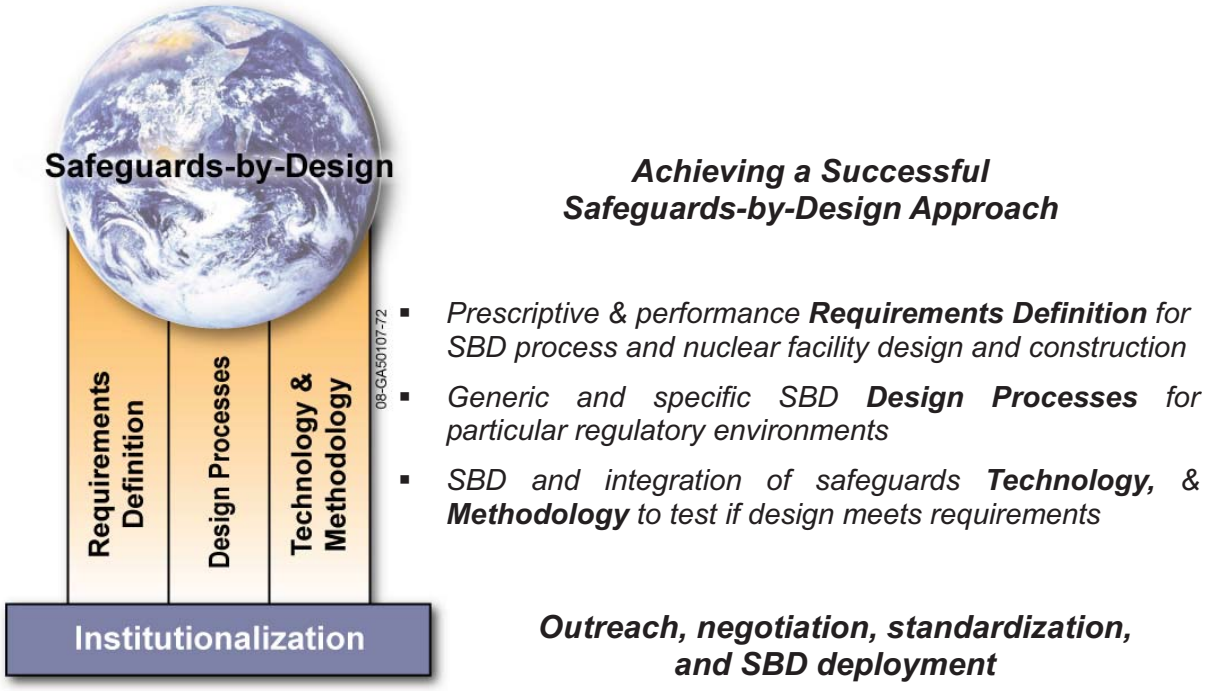


Fig. 2. High-level Framework to Institutionalize Safeguards-by-Design

The work discussed here 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. This was determined to consist of the foundation of Institutionalization, which supports three "technical" pillars {Requirements definition (Section 4), Design processes (Section 5), and Technology and methodology (Section 6)} that in turn support the pinnacle of achieving a successful Safeguards-by-Design approach. Beyond the goal of institutionalizing SBD in U.S. nuclear infrastructure development and design, as illustrated in Fig. 2, this work also contributes to international efforts to develop and institutionalize SBD as a global standard for the development of new nuclear energy infrastructure.

The proposed SBD process manages interaction between safeguards, MC&A, and security design and the overall design process, especially safety system and process design, to progressively develop definition and analysis at each design phase [3,4, 4].

3.3 Project Management of Design and Construction

The SBD process must normally be applied within a conventional project management process, as outlined here. 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 technical norms, 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 the needs of customers such as utilities, local authorities, States, and the IAEA [5], see Fig. 3.

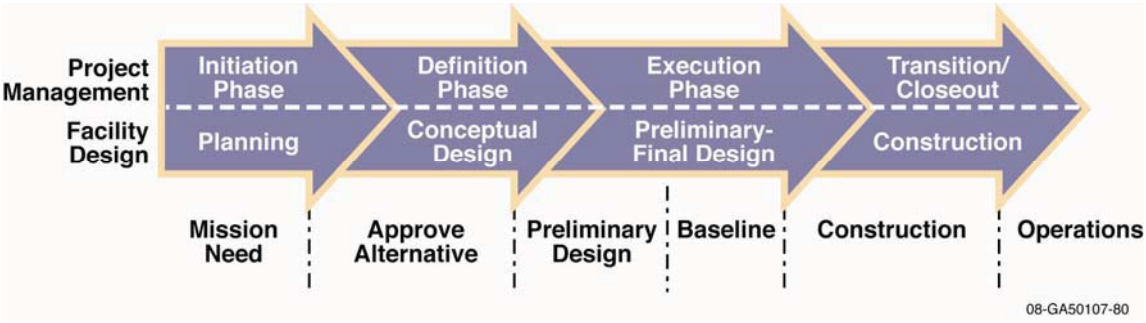


Fig. 3. Typical Phases of Project Management/Design [5]

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, security 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. 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 [6]. 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) or similarly “front end engineering design” (FEED). This illustrates the importance of the application of an SBD process where again the emphasis on early design involvement and requirements definition is all important.

4. SAFEGUARDS REQUIREMENTS

4.1 Overview

Definition of requirements, considered broadly to include guidelines, 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. Current approaches to establishing international safeguards concern mainly access to the facility and the nuclear material therein together with the performance of its monitoring and verification. By contrast, national physical security requirements tend

to be deterministic and relatively prescriptive. Requirements for advanced fuel cycle infrastructure, which will have substantial differences from current infrastructure in areas such as increased use of remote handling of materials, will need to increasingly evolve toward a more performance-based framework as has occurred for safety regulation. From the facility designer's viewpoint all requirements necessary for the successful execution of SBD must be formalized, and demonstrated methodologies, see Section 6, are needed to determine whether requirements are met by proposed designs. An assessment of the conceptual design to confirm that it meets, or has high assurance of meeting 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.

The area of guidelines and requirements is complex and dynamic, and different participants have differing needs and objectives. Requirements should be expected to evolve over time, both to address problems that may emerge with previous requirements, and also in the spirit of continuing improvement, as is the case for safety. Initially, due to institutional and technological developments always underway, guidelines, requirements and their acceptance criteria are unlikely to be fully agreed between organizations and not complete for the particular environment and facility planned. Guidelines may be negotiated at high level, e.g. between IAEA and SSAC, and turned into prescriptive or risk-informed design requirements for the specific facility by the owner/operator and/or vendor. The IAEA has criteria for safeguarding facilities and these can contribute to formulation of facility requirements. Prescriptive requirements, e.g. regulatory ones, may need interpretation for design purposes and performance requirements are often subject to commercial negotiation. The SBD process is part of the project management and design processes and is anchored by design requirements. The relationship of guidelines, requirements and criteria merits significant further attention.

4.2 Performance Requirements for SBD Process

The objective for institutionalizing the SBD process is to provide a procedure by which international safeguards, as well as national MC&A, physical security, and safety 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 other proliferation barriers of facilities in a cost effective way. 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 (as opposed to facility performance requirements) were formulated as follows:

a) Develop a simple, formalized, and integrated process for SBD that is beneficial to stakeholders
b) Develop the SBD process to be flexible, consistent with and enhance the effectiveness of applicable domestic and international directives, and compliant with relevant national and regional regulatory authorities.
c) Provide a useful tool for the project manager responsible for design/construction of nuclear facilities
d) Base the SBD process on accepted project management, design, and systems engineering processes
e) Provide safeguards and security in the facility providing maximum operational efficiency and lowest cost consistent with regulatory requirements and guidance
f) Mandate a concise set of project deliverables for safeguards and security design to demonstrate a systematic, comprehensive, auditable, and transparent project design
g) Develop phased safeguards effectiveness reports (akin to phased safety reports) to facilitate dialog with and acceptance by sponsors
h) Initiate safeguards and security design activities in the pre-conceptual planning phase through the establishment of a safeguards design team including security

i) Use systems engineering to integrate operability, safety, security, safeguardability, and other proliferation barriers into the facility design
j) Provide early identification of intrinsic design features that enhance safeguards, safety, security, or other proliferation barriers, or assist implementation of extrinsic measures
k) Mandate use of life-cycle cost (LCC) analysis as a criterion for capital expenditure decisions between intrinsic (early) and extrinsic (later) design alternatives

4.3 Prescriptive Requirements for the SBD process

The SBD process must comply with current national regulations, agreements, directives, etc. For example in the U.S., these include U.S. NRC, DOE, U.S. Code of Federal Regulations (CFR), and other national regulatory requirements for the nuclear fuel cycle. The facility, as designed, constructed, and operated must also comply with these and other requirements. National safeguards and security often covers such areas as: a. physical protection; b. material control and accountability (MC&A); and c. cyber security. The SBD process must also comply with international agreements related to non-proliferation, particularly with requirements for the implementation of efficient and effective IAEA safeguards. Although internationally accepted methodologies for assessing designs are still in development, progress is occurring in: d. proliferation resistance including the feature of safeguardability (see Section 6).

Proliferation resistance measures relate to the barriers that a proliferant State must overcome to acquire nuclear weapons through diversion from or misuse of infrastructure for nuclear energy systems. There are presently no formal national or international requirements for proliferation resistance that must be considered in design, and definition and acceptance of such requirements may take considerable time. However, the Generation IV International Forum's Proliferation Resistance and Physical Protection (PR&PP) methodology, and the IAEA-led International Project on Innovative Nuclear Reactors and Fuel Cycles, INPRO Manual – Proliferation Resistance, support the principle of including proliferation resistance in the design process [7,8]. Safeguardability is a property of the whole nuclear system and is estimated for targets on the basis of characteristics related to the involved nuclear material, process implementation, and facility design [7]. Both intrinsic and extrinsic features, including, importantly, safeguards, are included within the concept of proliferation resistance. Safeguardability, in turn, refers to the extent to which the design of the facility readily accommodates, and facilitates, effective and cost-efficient safeguards for the facility.

The proliferation resistance framework supports the SBD process by providing concepts and assessment methodologies for the quantification of the effectiveness of safeguards and security driven design in relation to lifecycle cost. This supports the iterative design process, see Fig. 4.

Countries, party to the Nonproliferation Treaty (NPT), conclude a comprehensive safeguards agreement with the IAEA to cover the construction, operation, and decommissioning of their nuclear facilities. Important IAEA documents, directly related to the agreement between the IAEA and States, which have acceded to the NPT, include:

- IAEA INFCIRC/153: The Structure and Contents of Agreements Between The Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons
- IAEA INFCIRC/274: The Convention on the Physical Protection of Nuclear Material
- Subsidiary Arrangement to the Safeguards Agreement (includes Facility Attachment)
- IAEA INFCIRC/225: The Physical Protection of Nuclear Material and Nuclear Facilities
- IAEA TECDOC-967: Guidance and Considerations for the Implementation of INFCIRC/225, The Physical Protection of Nuclear Material and Nuclear Facilities
- IAEA INFCIRC/540: Model Protocol Additional to the Agreement(s) between State(s) and the IAEA for the Application of Safeguards

The four main elements of the IAEA facility-specific international safeguards approach, see Fig.1, are the design information questionnaire, facility safeguards approach, facility attachment, and design information verification. Under the comprehensive (INFIRC/153-type) safeguards agreement, more detailed IAEA criteria include that nuclear facilities will have, use, or permit:

a) Defined "Material Balance Areas" to facilitate nuclear material accounting
b) "Key Measurement Points" for measuring the flow and inventory of nuclear material
c) Defined "Strategic Points" for the application of containment/surveillance and other safeguards verification measures
d) Nuclear Material Accountancy based on facility operating records and state reports
e) An annual Physical Inventory Taking and Verification, which is typically a complete physical inventory of all nuclear material in the facility
f) Verification of domestic and international transfers of nuclear material
g) An accounting process that will permit the IAEA to perform a statistical evaluation of the nuclear material balance to determine "Material Unaccounted For"
h) Routine (monthly or quarterly) "Interim Inventory Verifications" for the timely detection of the possible diversion of nuclear material
i) Verification of the facility design information (relevant to safeguards)
j) Verification of the facility operator's measurement system (relevant to safeguards).

Safeguards inspection criteria have been developed and codified by the IAEA based on the type of nuclear facility (e.g., power plant, uranium conversion plant, uranium enrichment plant) and are summarized in the Safeguards Criteria Section of the IAEA Safeguards Manual [9]. These criteria specify facility safeguards requirements additional to those in the Safeguards Agreement. The safeguards criteria depend on the type of nuclear material, whether irradiated or unirradiated, and closeness to direct use to produce a nuclear weapon. These facility-specific criteria must ultimately be translated into actual designed and engineered equipment and features in the facility to perform the requisite activities to the level as specified in the criteria. This poses a significant challenge to the designer in interpreting the IAEA Safeguards Criteria and formulating appropriate design requirements. The latter should lead to minimal but adequate facilities and minimize the impact on operational procedures and costs. To achieve these objectives, earlier and more complete interaction and collaboration between the facility designers, SSAC, and the IAEA is recommended [1].

5. SBD PROCESSES

5.1 Example of the SBD process within a National Regulatory Environment

Design processes for SBD 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 [5,6]. To initiate studies, the development of a proposed SBD process within a particular regulatory system was needed as an exemplar of a State environment. The use of the DOE regulatory environment was selected as the example study presented here due to existing knowledge, experience and the completeness, detail and availability of the directive system. The study generated a single proposed SBD process including identification and description of activities, deliverables, interfaces, and hold points covering both domestic regulatory requirements and international safeguards.

The conventional main phases of design, i.e. conceptual, preliminary and final, are shown in Fig. 3, and comprise cycles of safeguards activities which contain: design iteration (SBD design loop, see Fig. 4), review, risk/opportunity assessment, vulnerability assessment, cyber security plan, specification

development, effectiveness review, strategy development, and stakeholder response. Within each phase, the SBD process calls for the SBD team to receive design information from the overall facility project design, and perform a loop of specialized safeguards and security related design activities, see Fig. 4. These cover safeguards requirements definition, safeguards design, assessment of design effectiveness (or conversely vulnerability), re-iteration of design if needed, and exit to project design review when appropriate with subsequent repetition if needed. Collaboration with specialist design teams, such as safety, is required. The loop is graded in that design definition increases in each design phase whilst the overall pattern is repeated for comment resolution as necessary. There are iterations of the SBD design loop initially in the three main design phases, and lastly during facility construction, transition, startup, and closeout.

The proposed SBD process, for the example environment, develops an overall safeguards design strategy, which documents the design approaches that the project proposes to meet the domestic safeguards requirements from directives and performance requirements from vulnerability assessment, cyber-security planning, MC&A process analysis, and proliferation barrier analysis. The latter two are projected new analyses to support the early identification of the design features relied on to meet safeguards performance requirements. The MC&A process analysis identifies the design features and associated system performance requirements needed to meet the established nuclear MC&A standards, commensurate with the maturity of the design. This analysis is tailored to the complexity of the facility and the safeguards significance of the nuclear material housed at the facility. The second proposed analysis is the proliferation barrier/safeguardability analysis, see Section 6, which identifies the design features and associated performance requirements needed to meet intrinsic and extrinsic proliferation risk reduction requirements.

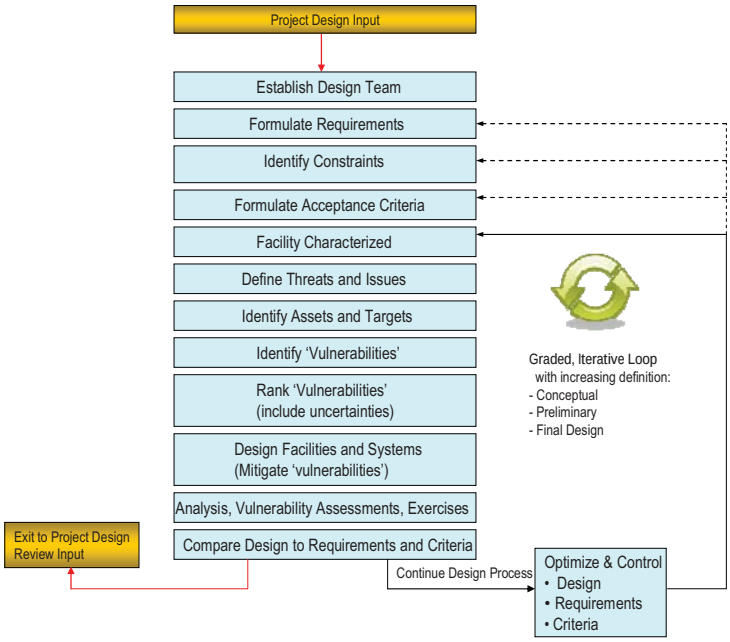


Fig. 4. SBD Design Loop.

The study was performed in two convenient but otherwise arbitrary stages: firstly, developing a process driven only by the combination of domestic requirements and SBD performance requirements and, secondly, modifying the first results to integrate the additional effects of incorporating international (IAEA) requirements. The study generated a proposed SBD process comprising 55 process steps, which included fourteen to account for the IAEA safeguards requirements (notably design information questionnaire, facility safeguards approach, facility attachment, and design information verification) and

forty-one in support of domestic requirements [4]. The SBD methodology adopted and the level of detail is comparable to that for integration of safety into the design process [10]. The step-wise approach was to simplify the study and facilitate its visual representation by means of two series of flowcharts [4]. Although new directives have not been drafted for use of SBD within the acquisition system, the SBD process is considered to be sufficiently developed to merit broader stakeholder review and be tested on a pilot scale for an actual project. These exercises would evaluate and improve process viability and help determine the best way to effect institutionalization within the regulatory structure.

5.2 Key Features of the SBD Process

Following the study of integrating the SBD process with that for design and construction management, the SBD project team extracted fundamentals [11]. The principal features were determined to be:

a) Early involvement of SBD team in the design effort
b) Early identification of safeguards, MC&A, and physical protection requirements
c) Early formulation of intrinsic features that will benefit the design
d) Closer integration of safeguards, MC&A, and security with project design leading to improved risk management, cost estimates and schedules
e) A clear and simple interaction plan between safeguards and the facility design process which identifies required activities and timeline and provides detail and analyses in each phase of design
f) Specific requirements for owner/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

In general, there is unlikely to be a unique “best way” to integrate design requirements and assessment methodologies, so that flexibility and judgment in application of the SBD process is important. 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 a range of States. 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 general project management sequence that might incorporate a variable number of hold points and could form a single path or comprise multiple parallel paths. This may bring increased flexibility to institutionalize SBD within the framework of any oversight regime.

6. SUPPORTING TECHNOLOGY & METHODOLOGY

6.1 Overview

Technology and methodology form the third technical pillar of the ISBD framework, see Fig. 2. This area includes development of technologies, including instrumentation and data processing, for better supporting safeguards approaches [12], and methodological toolkits for assessing facility designs for compliance with design requirements [13]. Other technological applications are the development of engineering standards and guidelines, some widely applicable to nuclear facilities and others to specific facility type, and the study of best practices and lessons learned for relevant nuclear facilities. The pursuit of improved precision and accuracy of measurement of material mass and isotopic content in various geometries, chemical and radiochemical environments, and phase dispersions is longstanding. Some assessment methodologies are under development and not yet well accepted by regulators and industry. Vulnerability assessment in relation to physical security is relatively well developed on a deterministic, prescriptive basis. Assessment of proliferation risk reduction, including safeguardability, is less well developed. As was experienced in the field of safety including the present trend toward probabilistic safety analysis, there is an expectation that full maturity will take significant time as implementing

authorities and technical experts gain experience. The SBD process has the flexibility to enable parallel process testing and methodology development. The emphasis in this Section is on the status of developments in proliferation resistance and the sub-topic of safeguardability.

6.2 Safeguards Objectives

The goal of international safeguards for nuclear facilities is to provide timely detection of the diversion or misuse of the facility to acquire materials for nuclear explosives. The safeguards system is subject to two distinctly different types of potential errors: Type I errors (false alarms/false positives), and Type II errors (non-detection of diversion or misuse). The plant operator, the State, and the IAEA all have a mutual interest in designing and operating facilities to achieve a low rate of false alarms (anomalies requiring an IAEA investigation) and a very low rate of false positives (where an IAEA investigation cannot confirm the absence of diversion or misuse, or incorrectly concludes that diversion or misuse has occurred).

The risk of false alarms and false positives will be dominated by safeguards failures that can occur due to off-normal, accident, and physical security events. The systematic identification of potential events and their potential frequencies is a central part of the design of the safety and physical security systems for nuclear facilities. Thus substantial benefits can come from closely integrating the design of the international safeguards system with the safety and physical security system design processes. Clearly, safeguards, safety, security, and reliability (process control) all benefit from an accurate and timely knowledge of the location of nuclear materials.

On the other hand, Type II non-detection errors do not result from random initiating events, but instead from the strategic decision of a State to divert material or misuse a facility. This distinction is important, because the State can be deterred from attempting diversion, even when the probability of non-detection errors is relatively large (say up to 10%), without generating much risk that diversion will be attempted. While in principle, a State could divert material ten times in order to obtain a reasonable probability of having one diversion go undetected, this is not a strategically rational behavior.

It is also important to note that the State, as a strategic actor, has the capability to alter the frequency of some types of initiating events to be larger than the normal rate, just as in the case of physical protection where the normal, random probability of different combinations of equipment or system failures can be changed by the strategic actions of an adversary.

Under SBD, the interlinkages between international safeguards, safety, and reliability are considered explicitly. This does provide the opportunity to design safeguards systems specifically to achieve very low rates of Type I errors, which benefits safety and reliability as well.

6.3 Proliferation Resistance Measures

Proliferation resistance is defined by the IAEA as “that characteristic of a nuclear energy system that impedes the diversion or undeclared production of nuclear material or misuse of technology by the State seeking to acquire nuclear weapons or other nuclear explosive devices” [14]. The term “proliferation resistance” relates to the host State as the threat, and greater technical capability is ascribed to the host State in carrying out a proliferant act than to a non-State adversary. It is essential to understand that no nuclear energy system can be proliferation proof, but different systems can present varying degrees of proliferation risk that can be reduced by the combined actions of the proliferation barriers acting in that system, which make diversion or misuse technically more difficulty to carry out and more readily detectable. Institutions and States can erect and maintain institutional barriers to proliferation and examples of such extrinsic measures include treaties, commercial and legal arrangements, and export controls.

Designers can contribute to proliferation risk reduction through the selection of processes and incorporation of facility design characteristics, i.e. intrinsic features, which either directly impede proliferation pathways or facilitate the cost effective application of other extrinsic measures, like the activities associated with international safeguards. Intrinsic features include inherent physical properties of the system and are in general robust and desirable because they are very difficult to modify or overcome [7]. A nuclear energy system's proliferation resistance may vary according to the specific host State threat and results from the combined effect of all its different barriers. It results from the application of international safeguards plus other proliferation barriers. The incorporation of the latter in facility and process design can be readily implemented through the proposed SBD process. Ultimately the specification of relevant requirements will be necessary since project management systems do not allow designers to act in their absence although the vendor may follow a level of custom and practice. Future efforts should be directed at defining realistic requirements and establishing the methods by which system performance against these requirements can be assessed.

The proliferation resistance and physical protection working group of the Generation IV International Forum (GIF) proposed six high-level measures for proliferation resistance, which are useful already and continue to evolve [7]. The evaluation for proliferation resistance then involves a systematic search for potential proliferation pathways, evaluation of measures for these pathways, comparison of pathways, and iterative improvement of the system design to reduce the attractiveness of potential proliferation pathways. The measures are:

a) Detection Probability - The cumulative probability of detecting a proliferation segment or pathway.
b) Detection Resource Efficiency - The efficiency in the use of staffing, equipment, and funding to apply international safeguards to the nuclear energy system.
c) Proliferation Technical Difficulty - The inherent difficulty, arising from the need for technical sophistication and materials handling capabilities, required to overcome the multiple barriers to proliferation.
d) Proliferation Cost - The economic and staffing investment required to overcome the multiple technical barriers to proliferation including the use of existing or new facilities.
e) Proliferation Time - The minimum time required to overcome the multiple barriers to proliferation (i.e. the total time required for the project by the host State).
f) Fissile Material Type - A categorization of material based on the degree to which its characteristics affect its utility for use in nuclear explosives.

The first two measures relate specifically to the application of international safeguards to the nuclear energy system. The term safeguardability is used in the context of future nuclear energy systems and is defined as "the ease with which the system can be effectively and efficiently placed under international safeguards" [7]. These safeguards-related measures suggest the importance of designing facilities to make it easier to apply safeguards that are efficient and provide high detection probability for all potential proliferation pathways. Three further proposed measures describe other barriers presented by the system to the proliferator and suggest the design objective of making it technically difficult, time-consuming, and costly for the potential proliferator to exploit the nuclear energy system. The sixth measure, relating to the attractiveness of the material obtained from a proliferation pathway, is essentially established by the fuel cycle properties. It is important that all nuclear materials, which can be used in a nuclear explosive device, be subject to high standards for safeguards and security, and recently reported research indicates that a number of nuclear materials and grouped products are attractive for use in nuclear explosives [15].

6.4 Proliferation Resistance Assessment

The development of a mix of methodological approaches was initially proposed to define and assess the performance of nuclear energy systems of the future [14]. Progress has been made with a three-pronged methodological approach to assessment of proliferation resistance and physical protection; viz. checklist, qualitative, and quantitative approaches. The IAEA-led International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) program has developed the checklist approach [8], while GIF has pursued development of a risk-informed methodology for both the qualitative and quantitative assessment approaches [7].

The checklist approach considers specific system design characteristics or properties, one at a time. The GIF working group evaluation methodology on the other hand calls for a holistic, risk-informed analysis that examines the relative performance of whole nuclear energy systems. The two methodologies are useful today, are proving to be complementary in their use, and both continue to evolve [13]. The risk-informed analysis approach is particularly valuable as a tool for systematically identifying vulnerabilities of a system and in guiding the use of resources for their mitigation, whilst checklists provide increased assurance of completeness in analysis. For these reasons, a risk-informed, holistic analysis approach coupled with a systematic review of previous experience, like that advocated by the GIF working group, is particularly well suited for application in the SBD process.

Risk-informed analysis commonly uses the construction of event trees (or equivalent) to describe the possible strategies (pathways) that an adversary might exploit in order to achieve the desired objectives. For preliminary work, the process of constructing and inspecting the trees in a disciplined fashion, combined with expert judgment, is a practicable approach to identifying and estimating vulnerabilities and then allocating resources to mitigate them. This type of analysis is valuable during the conceptual design phase. As design detail increases the definition of the events considered changes accordingly. As design progresses, more rigorous, quantitative analysis of performance of the system as a whole takes place including assessment of uncertainties. This graded, iterative approach to SBD as proposed here is illustrated in Fig. 4. It is not yet clear what extent of application of such methodology will prove to be economically justified.

GIF has continued to develop its methodology with the aid of a series of studies. The example sodium fast reactor (ESFR) consists of four sodium-cooled fast reactors of medium size co-located with an on-site dry fuel storage facility and a pyrochemical spent fuel reprocessing facility. The objectives of the case study were to exercise the GIF proliferation resistance and physical protection methodology for a complete Gen-IV reactor/fuel cycle system; to demonstrate, via the comparison of different design options, that the methodology can generate meaningful results for designers and decision makers; to provide examples of evaluations for future users; and to facilitate other ongoing collaborative efforts (e.g., INPRO) and other national efforts [16,17]. Consistent with the foregoing, it was found that structured qualitative analysis can produce traceable, accountable, and dependable results providing useful information to system designers, and when applied at the conceptual design level can aid in the development of functional requirements for SSC, which can guide subsequent detailed design.

7. BENEFITS AND CHALLENGES

SBD has the 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. There is a wide range of technologies and facility types used within the nuclear fuel cycle including defense facilities. These have differing safeguards, safety and security aspects, which span emphasis on stability of operation to security of material, held. The basic SBD approach is expected to be applicable, with

adaptation, to all nuclear facilities regardless of the State regulations or directives governing their design, construction, and operation. Although national regulatory environments differ, the same basic decisions need to be made and the same basic management processes are required. SBD brings focus to State needs to include international safeguards aspects within facility acquisition and design, and also enables IAEA to bring attention to its requirements to conduct international safeguards including verification activities in an economical, reliable manner for the facility owner/operator. Particularly through focus on intrinsic safeguards features, SBD is supportive of recent U.S. NRC policy for advanced nuclear energy systems that requires concurrent consideration of safety and security requirements, while designing a facility, resulting in an overall security system that requires fewer human actions [18]. SBD has the potential to provide the greatest benefit for innovative designs, i.e. designs for facilities with new processes and/or new product and waste streams, where technological experience on which to base the selection of major options, such as process flow-sheet, equipment selection, and facility layout, is limited.

The authors believe an SBD process can be usefully applied today, within a nuclear facility design process, with tangible benefits for most projects by tailoring the process to the applicable regulatory environment. However, use of the proposed SBD process may need the introduction of formal requirements, e.g. regulations, or industry initiatives based on firm evidence of value, such as pilot testing or demonstrations. These do not yet exist given the early stage of development. Tests or other activities, that illustrate the benefits of applying the SBD process, could be of particular value. Other challenges remain. The SBD process relies on the incorporation of international safeguards, MC&A, security, and safety requirements stemming from existing treaty commitments, laws, regulations, stakeholder interests, industry standards, political will of a State for transparency, etc. Where safeguards related guidelines or requirements are incomplete, or difficult to translate into meaningful design requirements, they must be improved or replaced. There are no broadly agreed design standards or formal design requirements for proliferation risk reduction beyond those for international safeguards. Other barriers to the successful deployment of the SBD process include the lack of a comprehensive safeguards culture, use of differing terminologies, intellectual property concerns, the sensitive nature of safeguards and security information, differing nationality and clearance of international architect-engineer staff, and the potentially divergent or conflicting roles and interests of participating organizations in the process. Efforts to institutionalize SBD must address these major issues.

8. CONCLUSIONS

1. The authors believe that the development and application of a Safeguards-by-Design (SBD) process for new nuclear facilities has promise to reduce nuclear security and proliferation risks, and enhance safety in an economical way, while raising operational efficiency. Done properly, SBD has excellent potential to benefit all stakeholders, including specifically the IAEA and the owner/operator.

2. International work, under the auspices of an IAEA workshop, explored SBD for international safeguards and sought a more collaborative approach that integrates these into the facility design process earlier than is presently done. The aim is to develop effective safeguards that save operating costs for both the Agency and facility operator.

3. The application of the SBD approach to meeting national requirements for nuclear material control and accountancy, physical security and safety will directly contribute to the success of the SBD process for international safeguards, and may even prove to be a prerequisite.

4. The proposed SBD process is considered to be adaptable to the needs of any State nuclear organizational structures, complementary to the proposed SBD process within the international safeguards environment coordinated by IAEA and supportive to the IAEA integrated 3S concept.

5. Components of SBD include requirements definition, design processes, and supporting technology and methodology. These improve the effectiveness and efficiency of the safeguards design process as part of nuclear facility design, construction, and operation.

6. The proposed SBD process 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 international consensus and adoption.

7. The center of attention of the proposed SBD process is the early inclusion of requirements, and the early identification of beneficial, e.g. intrinsic, design features. Current engineering approaches emphasize front end design since the possibility to significantly influence major design features, such as plant layout, SSC, and processes, largely finishes with the conceptual design phase.

8. 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 and matured. The IAEA workshop participants [1] and the authors view the development of design principles, guidelines, and best practices as a valuable near term addition.

9. 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.

10. The benefits of SBD should be recognized within the broader proliferation resistance context. This is because a gauge for how much proliferation risk reduction is being achieved in an SBD activity is needed to be able understand its relative value with regard to economic, operational, safety, and security factors. Furthermore, there is a need for continuing development of assessment methodologies for proliferation resistance and physical security of nuclear facilities. These methodologies are useful in design development, and for determining whether systems meet design objectives or requirements and can demonstrate proliferation risk reduction.

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, and Safeguards Campaign. They also acknowledge permission to publish from the DOE.

REFERENCES

1. IAEA, Facility Design and Plant Operation Features that Facilitate Implementation of IAEA Safeguards, SGCP-CCA, Report STR-360, February 2009.
2. U.S. DOE, National Nuclear Security Administration: Nuclear Nonproliferation, http://nnsa.energy.gov/nuclear_nonproliferation/nuclear_safeguards.htm , NNSA Next Generation Safeguards Initiative, 2009.
3. Bjornard T., Bean R., and et al., Safeguards-by-Design: Early Integration of Physical Protection and Safeguardability into Design of Nuclear Facilities, Paper #9518, submitted to Global 2009 International Conference, Paris, and Sept 6-11, 2009.

4. Bjornard T., Alexander J., et al., Institutionalizing Safeguards-by-Design: High-Level Framework; Volumes 1 and 2, Idaho National Laboratory, Report INL/EXT-14777, 212 pp., January, 2009.
5. U.S. DOE, Order 413.3A, Program and Project Management for the Acquisition of Capital Assets, July, 2006.
6. INCOSE, Systems Engineering Handbook, Guide for System Life Cycle Processes and Activities, Version 3.1, August 2007.
7. 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.
8. 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.
9. IAEA, Department of Safeguards: Safeguards Manual – Parts SMI and SMC, Safeguards Criteria and Annexes, Vienna, Austria, January, 2004.
10. U.S. DOE, Standard STD-1189-2008, Integration of Safety into the Design Process, March 2008.
11. Bean R., Bjornard T. and Hebditch D., Safeguards-by-Design: An Element of 3S Integration, International Symposium on Nuclear Safety, Paper IAEA-CN-166/067, Vienna, Austria, April, 2009.
12. Schanfein M., Science & Technology Challenges for International Safeguards, Proceedings of the INMM 49th Annual Meeting, 2008.
13. Pomeroy G., Bari R., et al., Approaches to Evaluation of Proliferation Resistance of Nuclear Energy Systems, 49th Annual Meeting of INMM, Nashville, TN, July 13-17, 2008.
14. IAEA, Proliferation Resistance Fundamentals for Future Nuclear Energy Systems, IAEA STR-332, IAEA Department of Safeguards, Vienna, December 2002.
15. Bathke, C. 2008. Further Assessments of the Proliferation Resistance of Materials in Advanced Nuclear Fuel Cycles. Presentation to NEA P&T Meeting in Mito, Japan, October 2008.
16. Bari R., Proliferation Resistance and Physical Protection (PR&PP) Evaluation Methodology: Objectives, Accomplishments, and Future Directions, Paper #9013, submitted to Global 2009 International Conference, Paris, September 6-11, 2009.
17. Khalil H., Peterson P., et al., Integration of Safety and Reliability with Proliferation Resistance and Physical Protection for Generation IV Nuclear Energy Systems, Paper #9396, submitted to Global 2009 International Conference, Paris, and September 6-11, 2009.
18. NRC, NRC Issues Advanced Reactor Design Policy, NRC News No. 08-189, October 14, 2008.