International Development of Safeguards and Security by Design of Nuclear Facilities and Processes

by David J. Hebditch, Sinclair J. Third, Jon P. Martin and Michelle Wise
UKAEA, The Manor Court, Harwell, Oxfordshire, OX11 0RN, U.K.

ABSTRACT

The application of safeguards and security by design (SBD) for new nuclear facilities has the potential to reduce security risks and proliferation hazards, whilst improving major plant design characteristics including operational efficiency and minimization of lifecycle cost. Overcoming delays to facility licensing may become a key feature. This is supportive of the expected significant future expansion of nuclear power generation consistent with low worldwide environmental impact. This paper reviews international work being conducted to develop a structured approach to ensure the timely, 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 paper analyzes developments being made by various nuclear sectors and organizations with the intent to improve communication and aid overall progress.

The paper also seeks to place SBD into the context of other integration approaches being applied to safeguards, safety and security, that more strongly affect later phases of the facility lifecycle. SBD applies to a wide range of facility types in the nuclear fuel cycle but in terms of applicability to design of new plants may have most immediate application to proposed new enrichment and recycling facilities. It examines studies of the SBD process for various regulatory environments and illustrates their differences. As with most design procedures, there is tension between complexity and readiness of adoption by designers, operator/owners and regulators since, as now judged by industry, SBD must show both facility improvements and cost savings for the operator. More fundamentally, increased weighting of safeguards and security aspects, including proliferation resistance of nuclear fuel cycle facilities, may possibly be accorded to selection amongst conceptual alternatives during the early stage of facility design. This may evolve as further facilities are constructed.

INTRODUCTION

Internationally, there is an increasing need and resolve to prevent the proliferation of nuclear materials. This will assist access to civil nuclear power and its part in mitigating climate change and resource shortages. In 2008, an independent Commission report prepared at the request of the International Atomic Energy Agency (IAEA) Director General noted that “The Agency’s roles in nuclear safeguards, safety, and security complement each other: measures to strengthen any of these “three S’s” can have important benefits for the others and all of the three S’s are essential to the future growth of nuclear applications.” [1]. The U.S. Department of Energy (DOE) National Nuclear Security Administration (NNSA) recently undertook a review of international safeguards “which concluded that a comprehensive initiative to revitalize the international safeguards technology and human resource base by leveraging U.S. technical assets and partnerships was urgently needed to keep pace with demands and emerging safeguards challenges.” NNSA launched the Next Generation Safeguards Initiative (NGSI) to develop the policies, concepts, technologies, expertise, and infrastructure necessary to sustain the international safeguards system as its mission evolves over the next 25 years. Regarding the deployment of new types of reactors and fuel cycle facilities, and the corresponding need for development of new concepts and approaches, NGSI will apply a system-level approach to safeguards and promote “Safeguards by Design” as an international standard [2]. In the U.K., Her Majesty’s Government considers that nuclear security is a vital additional pillar to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) to provide greater

assurance against the risks from nuclear terrorism [3]. The U.K. aims to act as an exemplar in managing its nuclear fuel cycle and further develop and promote proliferation resistant nuclear technology to enable the safe expansion of civil nuclear power globally.

It is clear that the period up to the NPT Review Conference in May 2010 is a particularly important period to make progress with international partners on safeguards and security methodology and proliferation resistant technology, processes, and techniques.

EVOLUTION OF INTEGRATION OF SAFEGUARDS, SAFETY, AND SECURITY

Several decades ago, the work of "design" was considered to fully take account of safety, for example, the formative DOE sponsored text "Engineering for Nuclear Fuel Reprocessing", [4] states "In designing a plant that will successfully recover and purify the valuable materials from spent nuclear-reactor fuel, the design engineer has two limitations, *safety* and economy." Since then, plant complexity and/or scale has increased and safety has become a distinct and expert discipline that is undergoing fuller re-integration with facility design; for example, through directives and procedures, application of risk-informed, performance-based approaches, or the use of documented principles and best practices, etc. Through experience in the acquisition of major defense facilities, the U.S. Defense Nuclear Facilities Safety Board (DNFSB) and the U.S. DOE have found the need to formally integrate safety in design and a DOE Standard has been published [5]. Several DOE Sites have reported on their initial experiences, which has been a catalyst for the development of a proposed SBD process.

International safeguards are the technical measures, with a political objective, to deter and detect the misuse of nuclear facilities or the diversion of nuclear materials from civil to military use. At the wider level, international safeguards and security cover proliferation resistance, international safeguards and national safeguards and security. At the national level, safeguards and security have been defined as a system of physical protection, material accounting, and material control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of nuclear materials. Material control measures are generally "intrinsic" (inherent properties, physical and/or process design features) or "extrinsic" (institutional, legal and/or operational arrangements). In this paper "integration of safeguards" means "the activity of fitting together appropriate aspects or parts of safeguards and security that work well together and form an optimized system". The integration of domestic safeguards and security, for example, accountability, material control, physical protection, process, data handling and quality control with international safeguards has been proposed in various ways for several decades. In general, domestic safeguards and physical security have remained distinct entities, each with their own regulations.

Safeguards and security comprise or are affected by many inter-related aspects or parts. There are various approaches to integration of these, which can use subsets of the full set of factors depending on government priority, history, organization, directives, regulations, culture, technology development, rate of construction of new plants, economics, etc. Historically, it has been common to divide national safeguard activities into two wide categories: security (physical protection) and material control and accounting (MC&A), which in the U.S. have been regulated or licensed as separate entities by DOE and the U.S. Nuclear Regulatory Commission (NRC) respectively. Alternative high-level integrated safeguards concepts have included use of a single DOE office for safeguards and security and use of a single performance-based (as opposed to the normal prescriptive approach) order to cover both security and MC&A [6]. Analogously, the use of a single 10 CFR Part has been proposed for commercial licensees to reduce potential regulatory inconsistencies and streamline compliance by the licensee. None of these has been taken to date. A potential endpoint is the unification of all activities into a single system but this may be excessively complex and, a priori, is not necessarily the optimum.

Since the turn of the millennium, the term "integrated safeguards" has taken an additional particular meaning as the current IAEA safeguards system based on design and implementation of state-level integrated safeguards approaches making use of an optimized combination of measures available under the Comprehensive Safeguards Agreements (CSA) and the Additional Protocol (AP) [7].

Recently, the Generation IV International Forum elaborated the definition of safeguards and security as PP (physical protection) robustness and PR (proliferation resistance); the former relating to threats from sub-nationals and the latter from owner nation-states [8]. GIF identified an evaluation methodology for PR & PP. The IAEA has performed related studies concerning proliferation resistance assessment methodology [9]. Both approaches endorse the need for proliferation resistance considerations to be taken into account as early as possible in the design and development of a nuclear energy system. These have been compared and the strength and weaknesses of proliferation assessment concepts examined [10].

Formalization of the integration of safeguards and security, together with safety, into the design process, i.e. "safeguards and security by design", has been proposed and potential methodology identified recently [11-13]. It can make use of various proliferation resistance and physical protection/vulnerability assessment methodologies. This approach is being developed at the international level through an IAEA workshop and for U.S. national application through NGSI. The U.S. Energy Facility Contractors Group (EFCOG) has examined security and safety integration in relation to DOE nuclear facilities. In licensing U.S. commercial facilities, NRC has recently emphasized the integration of safety and security (including nuclear safeguards). A generic SBD process has been identified for wide potential application.

The Health and Safety Executive (HSE) is responsible for shaping and reviewing regulations, developing policy, producing research and statistics and enforcing the law relating to health and safety in the U.K. HSE regulates the nuclear industry through its Nuclear Directorate (ND). The Directorate's primary goal is to ensure that those it regulates have no major nuclear accidents. It is responsible for the U.K. safety regulation of nuclear power stations, nuclear chemical plants, decommissioning, defense nuclear facilities, nuclear safety research and strategy [14]. Since April 2, 2007, ND assumed responsibility for civil nuclear operational security and safeguards matters respectively through the Office for Civil Nuclear Security and the U.K. Safeguards Office. The U.K. has a nuclear safeguards system based on a best practice approach to actions in early design, which is outlined later.

IAEA SAFEGUARDS BY DESIGN

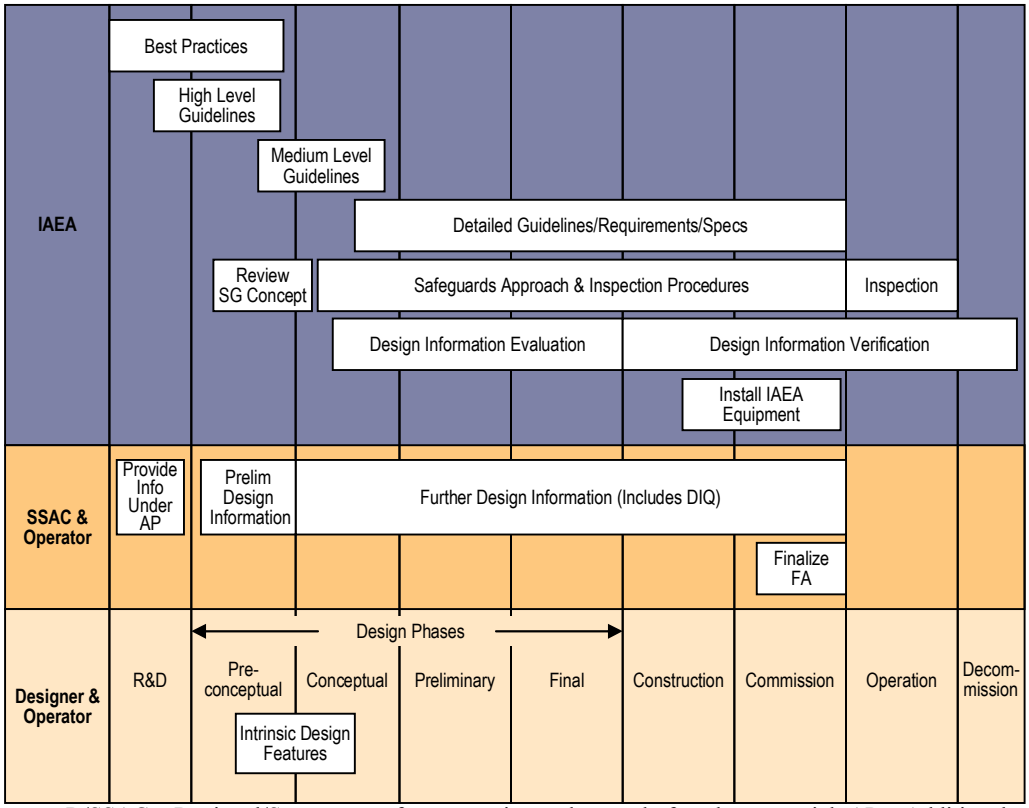
The IAEA emphasizes the complementary aspects of safeguards, safety and security [1]. The Agency understands *Nuclear safeguards* as the means applied to verify a State's compliance with its undertaking to accept an IAEA safeguards agreement on all nuclear material, in all its peaceful nuclear activities, and to verify that such material is not diverted to nuclear weapons or other nuclear explosive devices. IAEA has an international advisory role for *Nuclear safety* which is defined as 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 covers the protection of people and the environment against radiation risks, and the safety of facilities and activities that give rise to radiation risks. Similarly, IAEA promotes *Nuclear security*, defined as 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. It includes 'physical protection' as understood from consideration of the Physical Protection Objectives, Fundamental Principles, etc. Using separate INF/CIRC documents, IAEA defines two systems covering safeguards [15] and security [16], which possess differences and synergies.

For international safeguards, the detection of undeclared nuclear materials and activities is the greatest present-day challenge to provide assurance of the completeness of a State's declaration as well as its

correctness for the activities declared. The IAEA is adopting a flexible framework to tailor fit-for-purpose measures for each State. Some contextual differences from integration relating to national safeguards are that the IAEA may have more limited resources (per facility), restricted access and powers, and perhaps meet situations of extreme collusion not credible in the national safeguards context. Significant to facility design and facility-specific safeguards considerations, IAEA [17] drew attention to the chain:

Process/Technology →Diversion/Misuse Scenario → Detection/Safeguards Needs → Design Requirements (including Intrinsic features that facilitate the implementation of safeguards)

Concerning SBD, a workshop entitled "Facility Design and Plant Operation Features that Facilitate the Implementation of IAEA Safeguards" was held in October, 2008, at IAEA Headquarters in Vienna, Austria, with participants from Member States, the European Commission, the nuclear industry, and the IAEA [18]. The participants formulated a proposed IAEA SBD process as an approach where international safeguards are fully integrated into the design process of a nuclear facility, see Fig. 1.



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

Fig. 1. Proposed Safeguards by Design Activity Outline during Project Phases [18]

The IAEA is using the results of the workshop to develop guidance for designers and operators of nuclear fuel cycle facilities on the plant design features that facilitate the effective and efficient implementation of international safeguards. It was concluded that a disciplined application of project management and systems engineering during the phases of the facility lifecycle is essential. This commences in the research and development phase with a statement of safeguards requirements between the IAEA, the R/SSAC, operator, and designer. The Regional or State system for accounting and control of nuclear material (R/SSAC), in turn, provides the IAEA with preliminary design information. The proposed new process extends longer with increased collaboration. Another beneficial characteristic is the implementation of

intrinsic design features providing efficient and effective safeguards, while reducing operating costs. The workshop identified three categories of facilities depending on their state of development and deployment: existing; evolutionary; and developmental. The greatest impact of SBD is on developmental facilities where new design features and technologies may offer increased safeguardability, defined as the ease with which a system can be effectively and efficiently put under international safeguards [8], and need novel safeguards approaches. A further iterative process applying to the later phases of design/construction, using the design layout and relating to fully independent IAEA equipment and joint use equipment, has also been proposed [13].

Facility designers supported the concept but sought quantitative demonstration of overall cost reduction. Ideally the IAEA SBD process would be integrated into the existing national regulatory framework for nuclear safety and security and avoid extending the facility acquisition schedule [19]. There was strong support for earlier involvement of safeguards design than currently performed, to avoid costly redesign and project delays due to safeguards introduction after the design freeze. The better known safety in design model was welcomed as an analogy for SBD. There was a goal to issue a high level guide to international SBD in late 2009. Further discussion has since been published [20].

SAFEGUARDS BY DESIGN IN THE DOE REGULATORY ENVIRONMENT

Within the DOE, directives are the primary means for one Office to promulgate long term direction affecting other parts of the Department. The conventional separation of physical security and safeguards is employed using various directives. A small set of relevant ones is shown in Table I for illustration [21].

Table I. Selected DOE Directives [21]

DOE P 470.1	Integr Safeguards & Security	DOE O 470.3B	Graded Security Protection
DOE O 142.2A	VOA & AP with IAEA	DOE O 470.2B	Independent Oversight
DOE M 470.4-2	Physical Protection	DOE M 470.4-3	Protective Force
DOE M 470.4-6	Nuclear Material Control & Accountability	DOE M 470.4-7	Safeguards & Security Program References
DOE O 413.3A	Program/Project Management for Acquisition Capital Assets	DOE M 413.3-1	Project Management for Acquisition of Capital Assets
DOE G 413.3-1	Design-Construct with Systems Engineering with O 413.3A	DOE G 413.3-3	Safeguards and Security for Program/Project Management

An example of an area providing integration between physical protection and material control is in Chapter III of Section A, Materials Control, of DOE M 470.4-6 Chg 1. Also DOE O 413.3A, Program and Project Management for the Acquisition of Capital Assets, pages 32-3, states that: “Safeguards and security refers to an integrated system of activities, systems, programs, facilities, and policies for the protection of classified information and/or classified matter, unclassified control information, nuclear materials, nuclear weapons, nuclear weapon components, and/or the Department’s and its contractors’ facilities, property, and equipment.” The same section also states that “In order to support overall project planning and design, *applicable safeguards and security requirements* must be identified at the earliest possible project phase.”, which is an important element within SBD. The order, DOE O 470.4A, Safeguards and Security Program requires that programs be developed and directives implemented.

In the mid 2000s following schedule delays and cost increases at several major DOE design and construction projects, the U.S. Defense Nuclear Facilities Board particularly emphasized the issues of identifying and resolving safety issues as early in the design process as is practical. The DOE Order 413.3 for Management for the Acquisition of Capital Assets, was revised so as to better address safety during design. A new Standard, “Integration of Safety into the Design Process”, DOE-STD-1189-2008 March 2008, was developed to accompany the revised order. DOE has also developed supplemental guides to support the Order including one concerning use of systems engineering [22], which is important to

integration. DOE assembled a significant team in 2006 with participation from most DOE Sites, Laboratories, EFCOG, and contractor subject matter experts. The essential elements included: key personnel identification, overall project strategy including safety integration, regulator involvement in safety-in-design decisions, and identification of the DOE Critical Decision 1 (CD-1) as the milestone by when major safety systems and design parameters should be defined. Several pilot studies for implementing STD-1189 were performed at major facilities including BWXT Y-12 at Oak Ridge [23], IWTU at Idaho [24] and Sludge Treatment Project and Solid Waste Processing Facility at Hanford [25].

Important features of the Standard [5] include:

- Integrated (federal and contractor) Project Teams (IPT), and a contractor Safety Design Integration Team (SDIT);
- Safety Design Strategy (SDS) which describes how important safety issues will be addressed in the design and in development of key safety documentation;
- Development of facility-level design basis accidents for classification of important safety functions showing safety expectations for safety structures, systems, and components;
- Preparation of Conceptual and Preliminary Safety Design Reports, and Preliminary Documented Safety Analysis, for DOE approval before next design/construction phase; and
- Risk and Opportunities Assessment examining the risks of proceeding at early stages of design (especially conceptual design) with incomplete knowledge or assumptions.

The Standard provides a valuable two-page summary after the preface entitled "Safety Design Guiding principles" and many of these have analogies for SBD, see Table II for examples.

Table II. Examples of Analogies between Safety in Design and SBD

Recommendations of DOE-STD-1189-2008 [5]	**Proposals for Safeguards and Security Guidance**
Control selection strategy to address hazardous material release is based on following order: ➢ Minimization of hazardous materials ➢ SCCs preferred to Administrative controls ➢ Passive SCCs preferred to mitigative controls ➢ Controls for multiple hazards ≈ cost effective	Control selection strategy to address nuclear material diversion is based on following order: ➢ Minimization of nuclear materials ➢ Intrinsic features preferred to Extrinsic ➢ Passive barriers preferred to security controls ➢ Barriers for multiple materials ≈ cost effective
Risk & Opportunity Assessment includes Safety in Design approaches for cost and risk strategies	Risk & Opportunity Assessment includes SBD approaches for cost and risk strategies
Critical Decision (CD) packages describe safety-item selection, bases/risks/opportunities, for in-formed risk decision-making by project authorities	Critical Decision packages give safeguard-security item selection, bases/risks/opportunities, for in-formed risk decision-making by project authorities
Project team established early in project cycle and includes appropriate expertise	Project team established early in project cycle and includes appropriate expertise
Important safety functions addressed during conceptual design	Important safeguards and security functions addressed during conceptual design

An effective process for implementing SBD needs requirements definition, design processes, safeguards technology and assessment methodology, and institutional deployment. The emphasis of an internationally deployable SBD process is on the early design phases, safeguards design assessment, selection of major design options, intrinsic safeguards features, life-cycle cost assessment, safeguards and security case, risk management, and design and risk communication with major stakeholders. It is applicable to both the national (domestic regulator and operator) and international (IAEA) approaches to SBD but there are differences stemming from the differing roles and duties of these organizations.

An NNSA sponsored team from the U.S. national laboratories developed a proposed SBD process for the DOE regulatory environment [11,12]. A systematic series of steps was identified to fully integrate international and national safeguards, physical security and proliferation risk reduction into the DOE directives system governing facility acquisition. The phases and critical decisions of the acquisition system are shown in Fig. 2 [26].

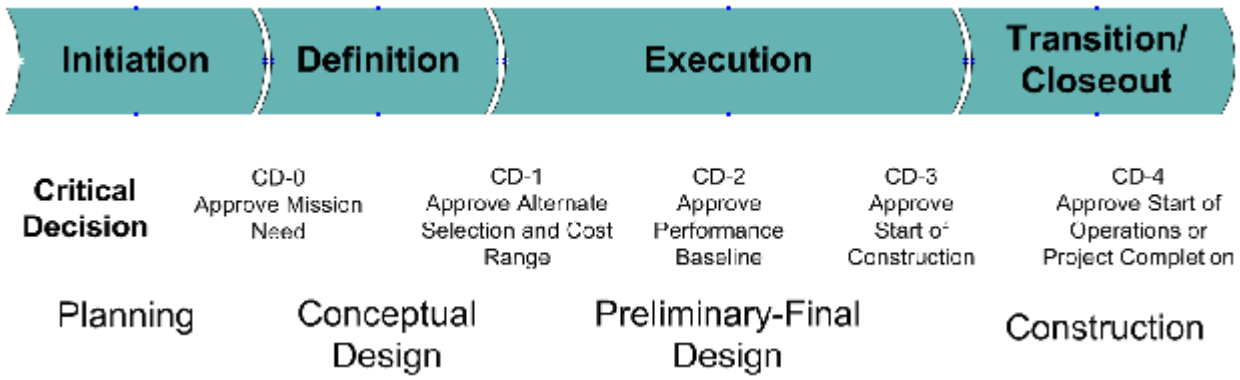


Fig. 2. Typical Phases of DOE Acquisition Management System [26].

For example during conceptual design, the proposed process specifies the formation of an SBD team, which provides safeguards and security requirements to the project functional and operational requirements. Following assessment of these by the project, the SBD team performs design activities which are reviewed internally and then supplied to the project for overall evaluation. The DOE directives require that agreed IAEA safeguards and security requirements be met. Full SBD design activities and interfaces were identified and flowcharted in relation to the four phases of design between CD-0 and CD-4 [11]. The flowcharts show interactions between project management, project engineering and safeguards activities. In all some 55 safeguards design activities and their interactions were identified, which is comparable to the complexity expected under safety in design within the DOE system.

SBD, which applies especially to new facilities possessing developmental or new technology, appears complementary to work already performed under the Safety and Security Interface Technology Initiative, undertaken by EFCOG with input from NNSA, Defense Nuclear Security NA-70 [27,28]. A cost effective, comprehensive process was developed to simultaneously satisfy design basis threat (DBT) and safety basis objectives for security systems. The initiative focused on standardized upgrades to enable existing DOE facilities to meet more stringent standards. The development of a library, or toolbox, of standard safeguards and security measures was proposed with associated use of established security effectiveness and hazard analysis results, which may have already received regulatory approval in comparable facilities with similar threat environments. A lessons learned exercise concerning safeguards and security integration with safety analysis, which was linked to EFCOG experience and conclusions, was reported by the Savannah River Site for the K-Area Complex [29].

From the above work, a generic SBD process was developed by U.S. National Laboratories and is shown below, which is considered adaptable to most regulatory environments. This could be used to standardize the approach to safeguards and security design of new reactor systems and other fuel cycle facilities.

U.S. NRC SAFEGUARDS AND SECURITY LICENSING ENVIRONMENT

The U.S. Atomic Energy Act of 1954 as amended in NUREG-0980, requires that civilian uses of nuclear materials and facilities be licensed, and empowers the NRC to establish by rule or order, and to enforce, such standards to govern these uses to protect health and safety and minimize danger to life or property. The NRC defines safeguards as used in regulation of domestic nuclear facilities and materials as “the use

of material control and accounting programs to verify that all special nuclear material is properly controlled and accounted for, and the physical protection (also referred to as physical security) equipment and security forces. As used by the IAEA, verifying that the "peaceful use" commitments made in binding non-proliferation agreements, both bilateral and multilateral, are honored." Concerning safeguards (including security) regulation of commercial facilities by NRC, the relevant Codes of Federal Regulations, see Table III, include:

Table III. Selected Codes of Federal Regulations (CFR) [30].

10 CFR Part 11	Criteria & Procedures for Determining Eligibility for Access/Control over SNM
10 CFR Part 40	Domestic Licensing of Source Materials
10 CFR Part 50	Domestic Licensing of Production and Utilization Facilities
10 CFR Part 70	Domestic Licensing of Special Nuclear Material
10 CFR Part 73	Physical Protection of Plants and Materials
10 CFR Part 74	Material Control and Accounting of Special Nuclear Material
10 CFR Part 75	Safeguards on Nuclear Material – Implementation of US/IAEA Agreement
10 CFR Part 95	Facility Security Clearance and Safeguarding of National Security Information and Restricted Data

Although topics are codified separately, integrating cross-references are provided. Examples of these are as follows: Physical Protection (Part 73) is dealt with in a separate code to material control and accounting (Part 74) though with limited cross-references as needed. The regulations 10 CFR 74.51, 74.53 and 74.55, provide an example of specific areas, respectively MC&A, process monitoring and item monitoring, where there is evidence of integration. The NRC Regulatory Guide (RG) 5.74, Managing the Safety/Security Interface, June 2009 [31], provided the addition of Section 73.58 to 10 CFR Part 73 requiring licensees to assess and manage safety and security activities to ensure that these activities do not adversely affect each other and that compliance with applicable security requirements in 10 CFR Part 73 or requirements in 10 CFR Part 50 or 52, and related regulations regarding the safety of the reactor and plant operations, are maintained. This guide describes a method that the staff of the NRC considers acceptable for licensees to assess and manage changes so as to prevent or mitigate potential adverse effects that could negatively impact either plant safety or security. Part 75, Safeguards on Nuclear Material – Implementation of US/IAEA Agreement, covers installation information, material accounting and control, reports, installations designated for IAEA safeguards, and enforcement.

The NRC has already taken several steps to improve security at existing nuclear power plants, including adopting a rule in March 2007 requiring both existing and potential new reactors to defend against a more realistic threat. The agency also issued a February 2002 Order, requiring all existing nuclear power plants to develop and adopt mitigating strategies to cope with large fires and explosions from any cause, including beyond-design-basis aircraft impacts. The NRC voted in December 2008 to codify these requirements in a separate rule for all existing and future nuclear power plants.

In 2008, the NRC published an update to its policy statement on advanced nuclear power plant designs, which provided expectations and guidance on safety, security and preparedness-related issues so, as a matter of prudence, designers can address them early in the development of advanced reactors [32]. These included concurrent consideration of safety and security requirements while designing a facility, resulting in an overall security system that requires fewer human actions and features that prevent a simultaneous breach of containment and loss of core cooling from an aircraft impact, or that inherently delay any radiological release. In 2009, NRC confirmed that advanced reactors should use simplified, inherent, passive, or other innovative means to accomplish their safety and security functions and that these attributes should also be considered early in the design stage to achieve a more robust, effective safety and security posture for small- and medium-sized reactors [33].

During 2009, NRC has been consulting stakeholders concerning extending the current concept of the safety culture to a safety and security culture. NRC concluded that safety and security serve the same ultimate purpose of protecting people and environment and it is important to provide integration of safety and security. The recommendation was for integration of safety and security within one Policy Statement and to allow flexibility to address differences in how safety and security are managed [34].

A Non-Nuclear Weapons State party to the NPT is obligated to place its facilities under international safeguards and the particular interaction with IAEA is usually initiated through notification to build a facility. However, the United States as a Nuclear Weapons State is not similarly obligated. Instead it has entered into a Voluntary Offer Agreement (VOA) with the IAEA such that its eligible (non-defense) nuclear facilities may be placed under international safeguards, if selected by the IAEA. Selection of an eligible U.S. facility by the IAEA can be made at any time after it is placed on the eligible facilities list. In 2008, NRC provided a new final policy statement concerning advanced reactors, which includes new items to be considered during the design including security, emergency preparedness, threat of theft, and international safeguards [35]. This may well be performed using an SBD process. The facility will therefore more readily accommodate international safeguards should the IAEA later decide on its selection. However, designer/operators may wish to avoid front loading of costs during design and construction to accommodate the potential, but low, probability of later selection by IAEA.

In general, the approaches and examples described in NRC guidance provide a method of compliance for a particular purpose, but are not intended to be all-inclusive. Licensees may often employ alternative methods for implementing NRC regulations other than the approaches discussed, provided that such measures satisfy the relevant NRC requirements. Each licensee should account for site-specific conditions when determining the measures needed for compliance with the applicable requirements in 10 CFR. Many of NRC's present regulations are based on deterministic and prescriptive requirements which are not readily replaceable and are maintained, while risk-informed (R-I) and/or performance-based (P-B) regulations are being developed and implemented. Over the past 15 years, NRC has implemented several plans, i.e. Probabilistic Risk Assessment (PRA), Risk-Informed Regulation Implementation Plan (RIRIP), and then in 2007 initiated the Risk-informed (R-I), Performance-Based (P-B) Plan. NRC has published various regulatory guides and significant research in this area including a feasibility study for an R-I and P-B regulatory structure for future plant licensing [36].

Although NRC has not yet explored nor adopted a SBD process, its R-I, P-B based approach allows a license seeker or its contractors to adopt such an approach where it can be adequately justified. As indicated, NNSA under the NGSI has developed a proposed generic SBD process which may be adopted potentially for commercial use worldwide. This proposed generic SBD process is now described.

SAFEGUARDS BY DESIGN IN A GENERIC LICENSING ENVIRONMENT

Within the NGSI, a current NNSA objective concerns development of a more generalized SBD process applicable within the U.S. licensed nuclear industry and internationally. This proposed generic SBD process is based on a generalized project management basis independent of any particular regulatory environment and uses the few and simple phases of "planning", "design" and "construction". A listing of generic activities within these phases has been provided with around eight main activities identified within each phase [37]. A multi national laboratory team [12] judged that the key features of the proposed generic SBD process are:

- Participation by the SBD team from the beginning of facility design;
- Early identification of requirements for international safeguards, MC&A, physical security and other non-proliferation objectives;

- Early conceptualization and development of intrinsic safeguards and security features;
- Improved integration of international safeguards, MC&A, physical security and other non-proliferation objectives with project engineering;
- A clear and simple plan, which identifies the required activities and timeline and provides detail and analyses in each project phase, for ensuring effective interaction between international safeguards, MC&A, physical security, and the facility design process;
- Requirements and/or hold-points for owner and/or stakeholder approval of design approaches and associated risks at key decision points; and
- Adequate flexibility to incorporate all regulatory requirements into the design of nuclear facilities;

These may be summarized as falling within the general categories of process optimization, risk mitigation, and stakeholder engagement. As such, significant economic benefits may be realized.

The design and development of safeguards and security features, as undertaken from the beginning of project engineering, shows where there may be potential synergies or conflicts between safety and safeguards and/or security. Advantage may be taken, or conflicts resolved, at lower cost and schedule impact. The benefits identified in DOE-STD-1189-2008, Integration of Safety into the Design Process [5], for particular use within the DOE directives system, of early consideration of safety requirements and development of safety design features are also applicable to treatment of safeguards and security. The use of systems engineering provides a structured approach for development of trade-offs in areas of design interaction between safeguards, safety and security. Potential benefits of the proposed generic SBD process include [37]:

- Reducing nuclear security risks and proliferation hazards, and enhancing the safety of new nuclear facilities in an economical way, while raising operational efficiency;
- Assessing the trade off between intrinsic (mainly capital cost) and extrinsic (mainly operational cost) features using lifecycle cost analysis;
- Assisting stakeholders including the IAEA and the owner and/or operator;
- Creating an SBD process framework readily integrating with nuclear facility design processes;
- Creating the possibility of demonstrating feasibility and usefulness in pilot tests on current design projects;
- Raising the effectiveness and efficiency of the design process for international safeguards, physical security and MC&A, and for safety;
- Improving project risk management and reducing project cost and schedule risks;
- Conforming to almost all regulatory, project management, and engineering environments, across a wide range of nuclear facilities; and
- 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.

U.K. NUCLEAR MATERIALS ACCOUNTANCY SYSTEMS AND SAFEGUARDS

The regulatory framework, which provides specifically for the implementation of nuclear safeguards in the U.K., mainly comprises requirements under Euratom Safeguards, IAEA Safeguards, and Bilateral Nuclear Co-operation Agreements. The U.K. has developed a draft Guidance Manual for Nuclear Materials Accountancy Systems and Safeguards to support effective nuclear material accountancy and safeguards (NMAS), which is required under European and U.K. law, in order to comply with international obligations [38]. The manual provides policy, procedures and quality management system requirements; a defined management structure and responsibilities; demonstrably trained and competent personnel for material accountancy and safeguards; separate demonstrably trained personnel for physical

security; a breakdown of sites into control and accountancy areas; and on-going review and monitoring with assurance of meeting requirements including continuous improvement.

Under Section 6.2, the Manual contains some elements of SBD such that in relation to materials accountancy and safeguards for any new or refurbished facility, the Design Project Manager "seeks endorsement of provisions planned, and implements the agreed design provisions." He complies with the "U.K. Nuclear Industries Security Regulations 2003 and seeks advice from the operator's Security Manager before committing to new work or amendments to existing arrangements." Under sub-sections 8.8.1, Design Objectives and Control, "the operator ensures that NMAS requirements are provided for in the design and implementation of new or refurbished plant and that appropriate consultation takes place with relevant parties." "All NMAS design decisions are fully documented in a controlled manner." Sub-section 8.8.2, Notification of Basic Technical Characteristics, states that "full design characteristics relevant to the accountancy and safeguards of new installations must be reported in a declaration of basic technical characteristics (BTC), as required by the European Commission Regulation (Euratom) No. 302/2005, at least 200 days before the first receipt of nuclear material into the facility." "Provisions are needed for the Safeguards Regulatory Authorities to verify independently the safeguards arrangements and design information prior to active commissioning."

In 2008, under the auspices of the U.K. Nuclear Decommissioning Authority (NDA), a good practice conference was held in the U.K. on safeguards and nuclear material accountancy [39]. It covered physical inventory taking (PIT), emergency physical inventory taking (EPIT), and IT NMA systems. EPIT interacted with security, for example an attack on a complex, large plant where there may be material theft or dispersion, casualties, need for evidence gathering, extensive searches to establish inventory, and urgent information demands from senior managers, regulators, and other stakeholders.

DISCUSSION

The concept of integration of safeguards and security is not new but its formalization and implementation has been slow. This is largely because the majority of nuclear fuel cycle facilities were already in existence and/or there was insufficient appreciation of the need for implementing safeguards requirements. The synergies concomitant with integrating safeguards, safety, and security, are recognized above but challenges also arise. Each of the project disciplines should recognize the needs of their peers and establish a consensus whereby a design solution can be agreed. Concerns can be strongest when addressing security matters, and particularly where an RSAC is involved. The disclosure of security information to foreign nationals, and members of international bodies, can pose issues. A possible example is where a multi-agency overview of video feeds monitoring access controls and storage facilities would provide a single solution meeting security and safeguards needs, but would present apprehension in terms of controlling the potential audience. The security regimes pertaining to facilities holding large quantities of nuclear materials are not available beyond those with a need–to-know. In integrating the related disciplines, but particularly safeguards (with its international membership), awareness of these sensitivities is needed. A satisfactory compromise position can generally be reached, which is usually based on limited dissemination of information, confined to those with a need-to-know, backed by information controls and signed undertakings. Similar issues can be experienced when discussing safety matters, but are usually limited, as the relevant regulator is not usually supranational. However, it should be noted that many of these concerns are not new to SBD and occurred during the former pattern of separate treatment of safeguards and security and their later involvement in project design.

There seems little doubt that implementation of a formalized safeguards and security by design (SBD) process will strengthen its industrial acceptance including integration with another facility critical action, i.e. safety. At the first and simplest level, the increased front end loading of design and increased emphasis on systems engineering is expected to improve facility definition, reduce schedule and cost risk, and

minimize the need for facility rework and retrofit. At the second level, the increased attention to safeguards and security together with safety in terms of selection of facility alternatives such as facility layout is expected to provide improved identification of and protection for areas of practical importance, using intrinsic features (related to inherent or passive features in safety) such as:

- Optimized physical separation/redundancy of system design;
- Strengthening existing protection of safety systems;
- Improved security stemming from multiple use of existing massive safety features;
- Early identification of containment and surveillance system envelope;
- Easier access for maintenance/testing and nuclear material accounting; and
- Access restrictions for security reasons combined with safe access/egress.

At the third level, the use of a SBD process is considered to facilitate the general trend in facility licensing in the commercial arena toward a risk-informed, performance-based approach and away from a purely prescriptive safeguards and security environment. This focus, now being strongly established in the safety area, is considered to raise effectiveness whilst containing costs. It is frequently adopted by commercial licensees where choice of approach exists. A fourth level, with particular dependence on risk-informed safeguards and security assessment methodologies including design assessment of proliferation resistance, concerns the extent of influence on major alternatives selection, where establishing definitive cost benefit is likely to be crucial. Underground location of a reactor or fuel cycle facility may bring major security advantages. Use of massive concrete features such as reactor containment can have both safety and security importance, such as respectively mitigating fission product release to atmosphere during severe accidents, and reducing the effects of deliberate impact of aircraft or other terrorist missiles. Adoption of a uranium enrichment process, e.g. laser type, considered capable of reaching commercial reactor fuel feed level but not of sufficiently high enrichment of uranium to have proliferation implications. Under U.S. GNEP, bold efforts were made to redefine the product and waste streams to improve waste management by reducing waste lifetimes consistent with reducing the attractiveness of mixed actinide products (U-Pu-MA), e.g. reduced purity level, lowered fissile content, reduced ease of handling and increased ease of detection,. The latter may have higher ultimate costs than the established commercial back-end fuel cycle and has significant entry costs. There may also be further trade-offs between chemical flow-sheet, remote handling and maintenance and cell design with impact on proliferation resistance. Even if adequate cost/benefit were established for selection of these major alternatives for a particular facility, there is the issue of seeking worldwide adoption at a time when delays to new build will become a significant handicap to the “nuclear renaissance.”

CONCLUSIONS

1. By review of the development of various integrating approaches, the predominance of safeguards and security by design (SBD) is shown. Its origins stem from integration of safety into design and its evolution is toward participation in the 3S integration of safeguards, safety, and security is now sought internationally.
2. Safeguards and security by design is identified as a key development seeking to improve 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.
3. The importance of focused design requirements, integration of safeguards and security design within project engineering, and effective methodologies for design assessment is emphasized and these must be effective during conceptual design as well as in later phases.

4. Improved early safeguards and security design, including collaboration of IAEA, R/SSAC, Operator, and Designer, is expected to improve facility safeguards and security operations, construction/ commissioning schedule, project cost and reduce retro-fitting.
5. Proposed safeguards and security by design processes have been described for several national regulatory environments and include the cases of DOE directives, NRC licensing, U.K. Guidance, and a generic process suited to tailored application within almost any further regulatory environment or to use within a non-prescriptive environment such as a risk-informed, and/or performance-based approach, regulatory guide approach, etc.
6. Both safety in design and safeguards and security in design emphasize the importance of methodologies for evaluation of alternative design concepts at the conceptual design stage. Alternative selection for civil, process, mechanical, operational, etc options must depend on agreed design requirements including safeguards, safety, and security and the importance placed on these.

ACRONYMS

AP	Additional Protocol
CD	Critical Decision
CFR	Code of Federal Regulations
CSA	Comprehensive Safeguards Agreement
DIQ	Design Information Questionnaire
DNFSB	Defense Nuclear Facilities Safety Board
EFCOG	Energy Facility Contractors Group
EPIT	Emergency Physical Inventory Taking
FA	Facility Attachment
MA	Minor Actinide(s)
MC&A	Material Control and Accounting
NMAS	Nuclear Material Accountancy and Safeguards
NGSI	Next Generation Safeguards Initiative
NPT	Treaty on the Non-Proliferation of Nuclear Weapons
PIT	Physical Inventory Taking
PP	Physical Protection
PR	Proliferation Resistance
PRA	Probabilistic Risk Assessment
R-I, P-B	Risk-informed, Performance-Based
R/SSAC	Regional/State System of Accounting for and Control of Nuclear Material
SBD	Safeguards and Security by Design
VOA	Voluntary Offer Agreement
3S	Safeguards, Safety, and Security

REFERENCES

1. IAEA, Reinforcing the Global Nuclear Order for Peace and Prosperity – Role of the IAEA to 2020 and Beyond, Report by Independent Commission for Director General, May 2008.
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. U.K. Cabinet Office, The Road to 2010 - Addressing the nuclear question in the twenty first century, Command 7675, United Kingdom, July 2009.
4. J.T. LONG (Editor), Engineering for Nuclear Fuel Reprocessing, Section 12-1, p. 860, DOE sponsored text, first printed by Gordon & Breach 1967, second printing by American Nuclear Society 1978.

5. U.S. DOE Standard, Integration of Safety into the Design Process, DOE-STD-1189-2008, March 2008.
6. R.L. CARLSON, Integrated Safeguards: A 1988 Perspective, J. Nuclear Materials Management, pp. 10-19, January 1989.
7. V. BRAGIN, Integrated Safeguards: Status and Trends, The Nonproliferation Review, pp. 102-110, Summer 2001.
8. Generation 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.
9. IAEA, Guidance for the Application of Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual - Proliferation Resistance, Vol. 5, Final Report of Phase 1, 16-07-2007.
10. G. POMEROY et al, "Approaches to Evaluation of Proliferation Resistance of Nuclear Energy Systems," 49th Annual Meeting of INMM, Nashville, TN, July 13-17, 2008.
11. T.A. BJORNARD et al., "Institutionalizing Safeguards-by-Design: High-Level Framework," Volumes 1 and 2, Idaho National Laboratory Report INL/EXT-14777, 2009.
12. T. A. BJORNARD et al., "Safeguards-by-Design: Early Integration of Physical Protection and Safeguardability into Design of Nuclear Facilities," Paper #9518, Global 2009 International Conference, Paris, Sept 6-11, 2009.
13. T.A. BJORNARD et al., Improving the Safeguardability of Nuclear Facilities, J. Nuclear Materials Management, Summer issue, pp. 74-86, 2009.
14. HSE, Nuclear Directorate – Who we are, http://www.hse.gov.uk/nuclear/nsd1.htm , October 20, 2009.
15. IAEA, 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), 1972.
16. IAEA, The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), 1999.
17. E. HAAS, IAEA Safeguards and Proliferation-Resistance Nuclear Technologies, http://www.sipri.org/research/disarmament/nuclear/researchissues/strengthening_reduction/prnt_folder/haas , NATO-Russia Workshop, Carnegie Moscow Center, March 2008.
18. IAEA, Facility Design and Plant Operation Features that Facilitate Implementation of IAEA Safeguards, SGCP-CCA, Report STR-360, February 2009.
19. M. STEIN et al., Safety, Security, and Safeguards by Design – An Industrial Approach, Paper #9307, pp. 2262-67, Global 2009 International Conference, Paris, September, 2009.
20. R.S. BEAN et al., Safeguards-by-Design: An Element of 3S Integration, International Symposium on Nuclear Safety, Paper IAEA-CN-166/067, 10 pages, Vienna, Austria, April, 2009.
21. U.S. DOE, Directives, Regulations and Standards, http://www.directives.doe.gov/directives/read.html , 2009.
22. U.S. DOE Guide 413.3-1, Managing Design and Construction Using Systems Engineering for Use with DOE O 413.3A, 2008.
23. Wilson B., Implementing U.S. Department of Energy Standard 1189 for the Uranium Processing Facility at Y-12, http://www.efcog.org/wg/sa_sb/docs/workshop_presentations/SAWG-SB-110607/Att_U-Wilson_1189.pdf .
24. J. HARVEY, DOE-STD-1189 and IWTU, Idaho Clean-up Project Nuclear Safety, EFCOG Safety Basis, http://www.efcog.org/wg/sa_sb/docs/workshop_presentations/SAWG-SB-110607/Att_C-Harvey_1189.pdf , November 2007.
25. A. RAMBLE, Fluor Hanford's Approach for Advance Implementation of Draft Standard DOE-STD-1189-YR, http://www.efcog.org/wg/sa_sb/docs/workshop_presentations/SAWG-SB-110607/Att_B-Ramble_1189.pdf , Fluor Hanford, November 2007.

26. U.S. DOE Order 413.3A, Program and Project Management for the Acquisition of Capital Assets, 07/28/2006.
27. 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.
28. K.J. CARROLL et al., Safety and Security Interface Technology Initiative, EFCOG Safety Analysis Workshop, INL report INL/CON-07-12582, May 2007.
29. J. HEARN et al., Safeguards and Security Integration with Safety Analysis, Washington Group International Savannah River Site, http://sti.srs.gov/fulltext/WSRC-STI-2007-00179.pdf , 2007.
30. U.S. NRC, NRC Regulations Title 10, Code of Federal Regulations, http://www.nrc.gov/reading-rm/doc-collections/cfr/ , 2009.
31. U.S. NRC, Managing the Safety/Security Interface, Office of Nuclear regulatory Research, Regulatory Guide 5.74, June 2009.
32. U.S. NRC, NRC Issues Advanced Reactor Design Policy, NRC News No. 08-189, October 14, 2008.
33. U.S. NRC, Moving Safety and Security to the Front Edge of Design" Prepared Remarks for The Honorable Gregory B. Jaczko, Chairman U.S. Regulatory Commission at the Workshop on Small- and Medium-Sized Nuclear Reactors, No. S-09-28, October 8, 2009.
34. U.S. NRC, External Safety Culture Activities, http://www.nrc.gov/reading-rm/doc-collections/commission/slides/2009/20090527/ext-saftey-culture-act-51309.pdf , May 27, 2009.
35. NRC, Policy Statement on the Regulation of Advanced Reactors, Nuclear Regulatory Commission, 10 CFR Part 50, Federal Register/Vol.73, No. 199, Oct 14, 2008.
36. U.S. NRC, NUREG-1860, Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing, December 2007.
37. R.S. BEAN et al., Integrating Safeguards and Security with Safety into Design, 2009 Safety Analysis Workshop – Integrating Safety into Design, Energy Facility Contractors Group, Las Vegas, Nevada, U.S.A., May 8-14, 2009.
38. U.K. Guidance Manual for Nuclear Materials Accountancy Systems and Safeguards, Draft 5 – March 2008.
39. U.K., NDA, Good Practice Conference – Safeguards and Nuclear Material Accountancy, November 13-14, 2008, NDA report dated 19-11-2008.