Abstract

The IAEA has described the Safeguards by Design (SBD) concept as an approach in which "international safeguards are fully integrated into the design process of a new nuclear facility from the initial planning through design, construction, operation, and decommissioning." Often, international safeguards features are added following completion of the facility design. Earlier consideration of safeguards features has the potential to reduce the need for costly re-designs or retrofits of the facility and can result in a more efficient and effective safeguards design. The U.S. Department of Energy’s National Nuclear Security Administration (NNSA) initiated a project in 2008 through its Next Generation Safeguards Initiative (NGSI) to establish a global norm for the use of SBD. The NGSI SBD program is evolving in parallel with a similar effort at the IAEA, while taking into account the IAEA’s SBD achievements and future plans. The NGSI program includes DOE laboratory studies, international workshops, engagement with industry and the IAEA, and setting an example through its planned use in new nuclear facilities in the United States. Consistent with this effort, the NGSI program has sponsored “Lessons Learned” studies and the preparation of facility-specific SBD Guidance documents. The NGSI program also takes into account successes that the NNSA has had with implementing safeguards early into facility designs within the U.S. The purpose of this paper is the presentation of the most recent developments in SBD under NGSI within the U.S. as well as the presentation of “Lessons Learned” integrating safeguards into new nuclear facility designs of the U.S. Nuclear Security Enterprise (NSE), namely the Uranium Processing Facility (UPF) project at the Y-12 National Security Complex in Oak Ridge, Tennessee and to discuss its relevance to international safeguards.

Keywords: safeguards; safeguards by design; HEU

1. Introduction

The NNSA’s NGSI has a key goal of advancing the Safeguards by Design (SBD) process, concepts and approach that promote the incorporation of safeguards elements or features early in the planning and design process for a nuclear facility. From the NGSI perspective, SBD has four main objectives:

1. Design new civil nuclear facilities that meet national and international nuclear safeguards requirements and objectives,
2. Make implementation of safeguards at these facilities more effective and efficient,
3. Avoid costly and time-consuming redesigns, retrofits, cost overruns, minimize disruptions to operating facilities, and protect sensitive information, and
4. Design facilities so that misuse of the facility and/or diversion of nuclear material is more technically difficult and easier to detect.
As the potential for nuclear energy expands, more countries are looking to the nuclear fuel cycle to meet their infrastructure development need. In response, the International Atomic Energy Agency (IAEA) must adopt new safeguards strategies, methodologies, and technologies as well as inspection regimes to become more effective. The organizational demands and budget requirements for international safeguards must change as demanded by member states. The IAEA describes Safeguards by Design (SBD) as a “concept” in which international safeguards are fully integrated into the design process of a new nuclear facility from initial planning through design, construction, operation, and decommissioning phases.

Planning the most effective safeguards strategy for a country’s nuclear infrastructure will be accomplished by implementing the SBD process during conceptual design, carrying it through final design ensuring that an approved safeguards strategy is implemented for active operations, with eventual decommissioning authorized by a safeguards decommissioning and disposal plan. It is important to realize that safeguards in general and by extension, international safeguards, must be designed into a facility and implemented in a way that integrates requirements or elements of multiple disciplines as they are inter-related in many aspects and have inter-dependencies that can be leveraged during systems engineering of the design process that provides defense-in-depth and cost savings. This integrated strategy is the premise behind implementing SBD into the design process for new nuclear facilities.

With the increased nuclear security requirements in the various fuel cycle facilities, it is appropriate to consider and present what is currently being accomplished programmatically by the U.S. Department of Energy/National Nuclear Security Administration (US DOE/NNSA) in the area of new nuclear facilities and the implementation of safeguards design strategies. In the U.S., the NNSA has begun incorporating safeguards into the design process of the UPF, and integrating appropriate safeguards with certain aspects of physical security and safety systems to provide a unified and layered cost-effective system. The design of UPF needed to have transparency such that the requirements that potential new arms control treaties might impose can be fulfilled.

This paper does not provide an in-depth discussion or “how-to” integrate the disciplines of nuclear safeguards, nuclear safety, physical security, cyber security, information technology, or physical protection. It does present the current state of SBD as well as recent developments to encourage the engagement of industry for readiness in the deployment of new nuclear facility designs to meet the safeguards requirements of the IAEA.

2. NNSA National Security Complex, Uranium Processing Facility Project in Oak Ridge, TN

From 1943 to 1989, The United States (U.S.) Department of Energy (DOE) built and operated a complex of manufacturing facilities comprised of over 120 million square feet at 17 major sites. During this time, the nuclear weapons complex (NWC) produced and processed tons of unique products and materials. In the late 1980’s and early 1990’s, increasing concerns about health, safety and the environment prompted the temporary cessation of operations at many DOE facilities. With the ensuing collapse of the Soviet Union and the cessation of the Cold War, old and inefficient legacy facilities would be permanently closed. However, DOE still retained these shuttered legacy facilities along with the responsibility of ownership of the nuclear material contained within the facility walls. The Y-12 Complex, operated by B&W Y-12 for the National Nuclear Security Administration, in Oak Ridge, Tennessee, contains part of this legacy.
With the end of the Cold War, along with the requirements for compliance with the technical and administrative terms of international arms control treaties, the complex was scaled back. The events of September 11, 2001 emphasized the need to consider proliferation concerns and safeguards and security protection of nuclear materials within the U.S. as well as abroad. To ensure an adequate supply of material for national security missions such as nonproliferation and nuclear deterrence, non-defense programmatic use in research and development and the support of nuclear power generation, NNSA required new production facilities. Facilities may include fabrication, purification, down-blending, enrichment, separation or recycling. In any case, managing nuclear materials requires highly sophisticated safeguards and security measures.

Hence, NNSA needed at Y-12 the new Uranium Processing Facility (UPF) Project that has focused upon producing an overall Material Control and Accountability Safeguards Design Strategy (MCA-SDS) that is efficient and integrated into the facility structure, the various processes and control system, as well as the material management system. Here is a case where a United States NNSA/DOE facility used the application of safeguards by design principles to achieve safeguards, security and safety goals.

3. Focus of NNSA/U.S. Domestic Nuclear Safeguards

U.S. Domestic Nuclear Safeguards is focused primarily on the internal threat and requires the use of an engineered and integrated systems approach to Material Control & Accountability (MC&A) to prevent material from being intentionally or unintentionally diverted from within a process, process room, or Material Balance Area (MBA) during active operational hours when personnel are present and actively engaged in material processing. An MBA is a geographical area corresponding to a specific production process where the nuclear materials inventory can be controlled and known. A Material Access Area (MAA) surrounds all the MBAs and is different than the MBA. It forms an outer perimeter where materials are not allowed under normal circumstances and is protected by multiple means. An area encompassing all facilities’ outside perimeters is defined as the Protected Area (PA).

The protection philosophy of U.S. domestic (internal) nuclear safeguards is at the local level, i.e., where processing occurs or where material is contained. The protection philosophy is based upon sequential layers of both defensive and offensive protection applied in a manner where the failure of a single feature in a layer does not compromise the protection of the material. The safeguards protection features within a single layer must be effective and integrated with other features in that layer to the degree necessary to ensure the protection required due to the importance of the material.

3.1 Core Safeguards Program Elements

NNSA regulatory requirements require MC&A to verify that the material is located where it is supposed to be, and in the quantities stated and to provide auditable records for a facility. Measurement systems are required to quantify the amount of materials present. This is an excellent example of defense in-depth and the overlap of the material control and accounting elements within the MBA element. With engineered physical features in place within new facilities, the design of the MBA maintains the control of the material as part of its integral processing operation. The MBA is also a subsidiary account in the accounting database as required by regulatory reporting requirements. Thus, the system of checks and balances has been established by regulatory requirements and has proven to be an effective regulatory requirement of Nuclear Safeguards for many years.

Physical features and engineered systems provide defensive controls and containment. Elements of a system such as material measurement and detection mechanisms as well as material accountability methodologies at the MBA and sub-unit level provide an offensive capability to deter or detect the loss
of material. This methodology also provides an investigative capability to localize any losses inside and between MBAs during transfer operations were they to occur.

Given the various system requirements, design criteria, regulatory standards, and specifications, the opportunity exists to apply systems engineering practices to the design process in these new facilities and processes to fully integrate the MC&A systems required in a manufacturing environment that will capture safeguards by design. MC&A systems are not limited to new technologies, but encompass new methodologies as well. Systems of the future must utilize integrated technologies and methodologies along with safety, manufacturing and security systems.

3.2 Systems Engineering and Safeguards - Systems Engineering Goal

Systems Engineering (SE) is defined as a proven, disciplined approach that supports management in clearly defining the mission or problem; managing system functions and requirements; identifying and managing risk; establishing bases for informed decision-making; and, verifying products and services meet customer needs. The goal of the SE process is to transform mission operational requirements into system architecture, performance parameters, and design details. Systems Engineering is interdisciplinary and holistic in that it focuses on the entire project in defining stakeholders’ needs and the required functionality early in the conceptual design phase. It then proceeds with design synthesis and system validation, considering the system life-cycle.

Systems engineering is utilized:

- upon approval of mission need to analyze alternative concepts based on user requirements, risks, costs, and other constraints to arrive at a recommended alternative;
- in the Project Definition Phase to integrate requirements analysis’ risk identification and analysis, acquisition strategies, and concept exploration to evolve a cost-effective, preferred solution to meet mission need;
- in the Execution Phase to balance requirements, cost schedule and other factors to optimize the design, cost, and capabilities that satisfy the mission need;
- to integrate the design and safety basis; and
- to plan, implement, and complete a project.

3.3 Material Control & Accountability Structures, Systems, and Components Selection Strategy

The selection strategy to address MC&A measures is based on the following order of preference at all stages of facility design and operation. Consideration must be given to the type of facility (storage or processing). Additional considerations include personnel interaction in facility operations, i.e., (do they provide one level of protective measures that are not administrative).

1. Minimization of impact to personnel safety is the first priority.
2. Structures, systems, and components (SSCs) are preferred over Administrative Controls.
3. Passive SSCs are preferred over active SSCs.
4. Active SSCs are complementary to passive SSCs (consider type of facility).
5. Preventative measures are preferred over mitigative measures (i.e., response).
6. Integrated facility safety SSCs are to be considered and can be complementary (i.e., Criticality Safety, Radiation Protection, and Accountability).
7. Controls closest to the source (MBA or sub-unit) may provide protection to the largest population of material.

8. Integrated protective mechanisms that are effective for multiple control measures (i.e., containment, surveillance, access) can be resource-effective.

Interfacing MC&A measurement and material control SSCs provide significant leveraging opportunities where the multiple disciplines’ requirements can be met. Utilization of such opportunities also provides significant cost avoidance in addition to the enhanced support for the integrated systems effectiveness.

U.S. Domestic Nuclear Safeguards, Physical Security and the various safety disciplines often use similar terms and have common goals but different methods. The natural affinity between the disciplines is important and the systems engineering process will ensure those common goals are achievable through the iterations of alternative selection and the design decision process.

4. Integration of Disciplines for Safeguards by Design
3S – Safeguards, Safety and Security

Nuclear Safeguards focuses primarily on the internal threat to the nuclear materials and uses an engineered and integrated systems approach to MC&A to prevent material from being intentionally or unintentionally diverted from within a process, process room, or Material Balance Area (and thus the facility). The focus of this threat is primarily during active operational hours when personnel are present and actively engaged in material processing and transfer activities. The other elements of the 3S, security and safety, are needed to be balanced in any facility under DOE operations.

4.1 Integration with Security-In-Design

The Physical Security program is a mature program and an organizational counterpart of Nuclear Safeguards. Implementation of extensive requirements, practices and technologies have ensured the evolution of the physical and protective actions of the security discipline. The program takes a graded approach for the protection of the lowest level of government property or interests and layered to the most critical. Physical features and engineered systems provide defensive controls and containment. Material detection and measurement systems as well as material accountability methodologies at the MBA and Process Unit level also provide additional capabilities to deter or detect the loss of material. These systems will also localize any losses inside or between MBAs as well identify losses that were to occur during internal facility transfers.

These measures are designed for both normal and emergency conditions. The systems in place must be functional for both normal facility processing operations as well as during periods of anomalous conditions, when activities are outside of the normal conditions of operations. The integrated systems maintain an overlap of capabilities or redundancy of sensor input points necessary for a complete risk-based assessed coverage for the appropriate level of protection required for the material. This combined and integrated network ensures no single point failure can compromise the system either during normal operations or anomalous conditions. Appropriate technologies are selected to capture data into the appropriate modules of the Information Technology Network (ITN) for information.

4.2 Integration with Safety-In-Design

A Safety Design Strategy is required to guide the design and support the safety basis documents at each phase of the project. The safety design strategy provides the safety guidance policies, significant
discipline interfaces from a safety perspective, and the safety goal considerations as well as the safety basis.

The basic Safety-in-Design precepts are as follows:

- appropriate and reasonably conservative safety structures, systems, and components are selected early in project designs;
- project cost estimates include these structures, systems, and components; and
- project risks associated with safety structures, systems, and components selections are specified for informed risk decision-making by the Project Approval Authorities, and
- the methods by which safety SSCs are designated (either safety class, safety significant, or defense-in-depth) during project phases must be documented and justified.

4.3 Nuclear Safeguards Focus

The focus of nuclear safeguards for NNSA in the U.S. is at the local level, i.e., where processing and handling occur. Therefore, material containment measures include: MAA, MBA, gloveboxes, and where necessary, other material enclosures. Transfer pathways into and out of the MBAs and gloveboxes are identified. Systems must be in place to detect and assess the unauthorized removal of nuclear materials, consistent with graded safeguards, and to localize removal from authorized locations.

Defense in-depth measures work together in processing operations to:

- deter the removal of material by inside adversaries due to multiple observable and unobservable obstacles,
- alert personnel to unauthorized removal of material,
- quickly localize any removal if it does occur.

The measures are designed for both normal and emergency conditions. The systems put in place must be functional for both normal facility processing operations as well as during periods of anomalous conditions.

5. Information Technology Enterprise System – A Near Real Time System

A modern information technology enterprise system that implements a near real-time (NRT) system for the control and accountability of all materials used within a facility is required. This is especially true for nuclear materials. Near real-time reporting (NRTR) incorporates the delay elements of operational processes and events where quantitative data is obtained at KMPs by operations personnel and/or auto-upload capabilities and it is input into the information processing system. The information processing (internal) and data presentation as performed by the computer system is performed in real-time once the data has been manually uploaded by operations personnel or captured automatically through technological means. The data is then presented (output) in usable format for approved personnel for viewing and review.

A facility material enterprise system must be designed to work in concert with personnel such that abnormal situations are flagged (e.g., inappropriate transfers of quantities, materials, unauthorized
personnel performing transfers or inappropriate timing of moves). Thus, multiple types of measurements and their respective equipment types are required for the measurement and documentation for the transfer of materials between MBAs to meet regulatory requirements for an overall safeguards strategy in the protection of special nuclear materials. MBA boundaries provide one layer of Key Measurement Points (KMPs) in a defense in-depth safeguards strategy for the control of nuclear material within the facility.

The Information Technology (IT) Enterprise Control system is the overall backbone in a dynamic lean-pull production control system. Instead of listing the steps in job routings and expecting the operators to —push— the completed component to the next step of the manufacturing process in the production control system queue, the production control system will be able to recognize the state of overall manufacturing operations within the facility, including material in-process due to production requirements within material balance areas, individual glovebox production units and process cells.

Establishing this in-process production relationship between all process cells is part of the pull production system. Dynamic communication with each production operating group in the adjacent manufacturing step is paramount in establishing a somewhat smooth flow in a process as complex and unique as any future domestic material processing facility. The product manufacturing control system will maintain an active communication link with the adjacent production process steps directly connected to it supply chain. The system will signal the input side of the production sequence that the process is waiting for product input. The overall production sequence will be monitored for overall process loading and throughput quantities.

Certain active databases are expected to collaborate within the production control system to implement limited shared data requirements that are complementary between various disciplines. An example of this is a criticality safety and material control location information system within glovebox production lines. See Figure 8, IT Enterprise System Architecture.

Process manufacturing units, where data is obtained via scale or other device, are subject to material loading limits. The production control system obtains the data and maintains it in an active database as well as supplying the necessary information as historical records. The local active database for the process cell and process units will be manipulated as part of the production control system.

Using input and output parameters of weights and other data from specific locations and product/container ID’s queued from the production control system within an enclosed environment such as a glovebox line will actively provide a lower-cost, safe, and efficient limited information sharing material tracking database to enhance both criticality safety and material control needs. Container loading and material location within a production process will be provided to the production operators (and other approved personnel) within the active production control system without intruding on the respective disciplines’ historical database. A glovebox having its regulatory required safety, mechanical, operational and various other sensors and alarm systems in addition to the production database material warning limits at the local level will inject another layer of defense-in-depth for material safeguards in a modern processing facility.

6. Inventory Capabilities

Current Nuclear NNSA/domicile MC&A/Safeguards regulatory requirements are that processing facilities cease operations, clean-up and perform a complete inventory every two months to determine a facility material balance. For modern processing facilities, a —dynamic inventory accounting methodology is expected as the data input at the in-process measurement points are captured in —near real-time. A safeguards authorization basis must be provided for new facilities, and receive approval from the NNSA after undergoing a thorough assessment of integrated facility and system design evaluation and operations tests, procedure as well as personnel qualifications prior to the facility receiving nuclear materials. System performance criteria will be determined after testing and
start-up. Safeguards and Security (S&S) performance will be graded based upon fundamental principles of established and graded risk management criteria.

In addition to the integrated design strategy to meet the safeguards risk-based criteria, another goal of the SDS is to relax the inventory frequency of UPF after having proven integrated, operational, safeguards and security capabilities after a period of time. It is a secondary goal of the SDS to provide the guidance and foundation for an integration model leading to an annual inventory.

7. Lessons Learned

While the UPF is a part of the DOE/NNSA nuclear security complex and not a commercial facility, it offers lessons learned for the commercial nuclear industry. The outdated and oversized nuclear complex within the United States required the transformation of the nuclear materials production capabilities into a smaller, safe and secure enterprise. Health and safety risks, environmental concerns, and the end of the Cold War all contributed to the required transformation. New missions and programs ensuring an adequate supply of material for national security missions, along with nonproliferation and nuclear deterrence will be provided by new manufacturing facilities in the future. Managing nuclear materials requires safeguards and security measures to meet any threats posed by both the potential external or internal adversary. Hence, the systematic approach to implementing the 3S in UPF shows how commercial fuel cycle facilities such as enrichment and reprocessing could benefit by designing in safeguards and security with the safety requirements for operation.

Material Control and Accountability regulations contain minimal prescriptive requirements relating to design of domestic, government-owned nuclear materials processing facilities. Project management design guides require that engineering documents contain specific and measurable statements relating to systems requirements. In MC&A, technical regulatory standards have neither been compiled sufficiently to be design requirements, or are non-existent altogether. The progress made in UPF could assist in making safeguards-by-design more feasible.

Safeguards measures cannot be unlimited in scope or cost, based upon whatever the disciplines’ engineers want in a facility. Budgetary expenditures for design and construction are questioned if the regulations are lacking in defined and detailed requirements that engineers need to design the process systems. A Safeguards Design Strategy for domestic nuclear materials processing facilities based upon a core —framework of MC&A regulatory programmatic elements that also utilizes the prescriptive requirements of safety, health and physical security regulations is justifiable. Engineered, facility and operational performance enhancements will be relied upon to reduce administrative and production encumbrances, and thereby reduce operating cost.

The opportunity exists to integrate multiple regulatory requirements utilizing Systems Engineering in the design process. System performance criteria will be determined after testing and start-up of new facilities and process systems. Safeguards and Security facility performance will be graded based upon fundamental principles of risk management criteria established by federal auditors. The goals of the Safeguards Design Strategy are significant and provide an opportunity for a —true domestic Safeguards System in a new Category I/II nuclear materials processing facility, the Uranium Processing Facility in Oak Ridge, Tennessee.
References


