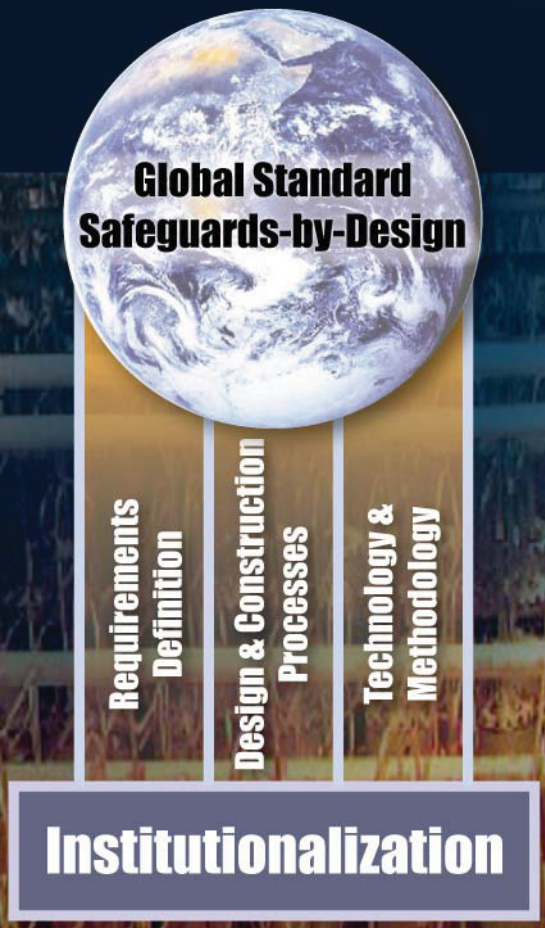
Institutionalizing Safeguards-by-Design: High-Level Framework

Volume 1



Trond Bjornard PhD (INL), Joseph Alexander (INL), Robert Bean PhD (INL), Brian Castle (INL), Scott DeMuth PhD (LANL), Phillip Durst (INL consultant), Michael Ehinger (ORNL), Prof. Michael Golay PhD (MIT), Kevin Hase PhD (LANL), David Hebditch DPhil (INL), John Hockert PhD (PNNL consultant), Bruce Meppen (INL), James Morgan (ORNL consultant), and Jerry Phillips PhD PE (INL)

Idaho National Laboratory

INL/EXT-08-14777 - Revision 1

Cover photograph of uranium gas centrifuge enrichment plant (Schanfein, 2008). The design of modern uranium gas centrifuge enrichment plants will benefit from application of the Safeguards-by-Design process.

INL/EXT-14777
Revision 1

Institutionalizing Safeguards-by-Design: High-level Framework

Volume 1 of 2

February 2009

Trond Bjornard PhD (INL)

Joseph Alexander (INL)
Robert Bean, PhD (INL)
Phillip Casey Durst (INL*)
Brian Castle (INL)
Scott DeMuth, PhD (LANL)
Michael Ehinger (ORNL)
Prof. Michael Golay, PhD (MIT)
Kevin Hase, PhD (LANL)
David Hebditch, DPhil (INL)
John Hockert, PhD (PNNL*)
Bruce Meppen (INL)
James Morgan (ORNL*)
Jerry Phillips, PhD PE (INL)

***Consultant**

Idaho National Laboratory
Idaho Falls, Idaho 83415

Prepared for the Department of Energy:
National Nuclear Security Administration
Office of International Regimes and Agreements (NA-243)
and
Office of Nuclear Energy
Advanced Fuel Cycle Initiative, Safeguards Campaign

EXECUTIVE SUMMARY

The application of a Safeguards-by-Design (SBD) process for new nuclear facilities has the potential to reduce proliferation risks as the use of nuclear energy expands worldwide. To this end a multi-laboratory team was sponsored in Fiscal Year 2008 to define a SBD process and determine how it could be incorporated into existing facility design and construction processes. The result could ultimately help form the basis for a new international norm for integrating international safeguards into facility design. This effort is a component of the U.S. Department of Energy's (DOE) Next Generation Safeguards Initiative (NGSI) and is jointly sponsored by the Office of Nonproliferation and International Security (NA-24) and the Office of Nuclear Energy. This is an interim report describing progress and project status as of the end of FY08.

Safeguards-by-Design means different things to different people. In this effort SBD is defined as a structured approach to ensure the timely, efficient and cost effective integration of international and national safeguards, physical security and potentially other nonproliferation objectives into the overall design process for a nuclear facility, from initial planning through design, construction and operation. A key objective is to ensure that security and nonproliferation issues are considered along with safety and other factors when weighing facility design alternatives.

The Institutionalizing Safeguards-by-Design (ISBD) team examined facility design processes, best practices and lessons learned from previous facility projects, developments in nuclear safety, and project and systems engineering, in order to identify the essential elements of SBD and a framework for its implementation. Historically, safeguards issues have been deferred until late in the design and construction process, resulting in added costs, and schedule and operational impacts associated with retro-fitting the facility. The application of a SBD process can help to reduce or eliminate these impacts in future facilities.

Central to the work completed in FY08 was a study in which a SBD process was developed in the context of the current DOE facility acquisition process. Since IAEA inspectors verify formal declarations made by the state, the project considered the incremental overlay of international safeguards requirements on top of requirements for a domestic safeguards system. DOE's current acquisition process already mandates certain steps relevant to SBD, for example, for physical protection and cybersecurity. The team identified the elements that must be added to support both the domestic security and international safeguards elements of SBD. The specific points in the DOE design process (see DOE O 413.3A, "Program and Project Management for the Acquisition of Capital Assets") where safeguards considerations must be taken into account were identified and are described in Appendixes E and G.

Modern design practices are increasingly front-end loaded, and the possibility to significantly influence major design features, such as process selection and plant layout, largely ends with the conceptual design step. Therefore SBD's principal focus must be on the early inclusion of safeguards requirements, and the early identification of beneficial design features.

The DOE study enabled the development of a "SBD design loop" described in Section 3 that is suitable for use in any facility design process. It is a graded, iterative process that incorporates safeguards concerns throughout the conceptual, preliminary and final design processes. Additionally a set of proposed design principles for SBD were developed and are presented in Section 4.

From the DOE study, a "Generic SBD Process" was developed and is described in detail in Section 6. Key features of the process include the initiation of safeguards design activities in the pre-conceptual planning phase, early incorporation of safeguards requirements into the project requirements, early appointment of an SBD team, 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 that domestic and international safeguards requirements are met, and formal communication of risks and management strategies to decrease the cost and schedule uncertainties. This

process, when fully developed, could help form the basis for an international norm for SBD as envisioned under NGSI.

The authors believe that the generic SBD process could be usefully applied today with tangible benefits for most nuclear design projects, within virtually any regulatory environment. However, the SBD process is unlikely to be broadly applied in the absence of formal requirements (e.g., regulations) to do so, or compelling evidence of its value. Neither exists today. A formal instrument to require the application of SBD is needed and would vary according to both the national and regulatory environment. Several possible approaches to implementation of the requirements within the DOE framework are explored in this report. Industry motivation to voluntarily embrace SBD will depend on the demonstrated benefits of doing so. Consequently, demonstrations or other activities that illustrate the benefits of applying the Generic SBD Process could be of particular value.

Other challenges remain. The SBD process relies on the incorporation of international safeguards and security requirements that derive from existing laws, regulations, stakeholder interests, industry standards, and elsewhere. To the extent that safeguards related requirements are incomplete, or difficult to translate into meaningful design requirements, they must be amended and improved. Also, there are presently no broadly agreed design standards or formal design requirements for proliferation risk reduction beyond those for international safeguards. Finally, there are numerous barriers to the implementation of SBD. These include the lack of a strong safeguards culture, intellectual property concerns, the sensitive nature of safeguards information, and the potentially divergent or conflicting interests of participants in the process. In terms of SBD implementation in the United States, there are no commercial nuclear facilities in the U.S. that are under IAEA safeguards and it is not clear whether the IAEA will select such facilities in the future. Efforts to institutionalize SBD must address these issues.

The authors envision a more ambitious set of objectives for the further development and implementation of SBD. The multi-decade long evolution of the risk-informed approach to safety provides a parallel that can illuminate the future development of the design approach to safeguards. Systems modeling and safeguards analyses offer a means for identifying vulnerabilities and evaluating efficient alternatives for addressing them. Further development and exploration would appear to be warranted, though the history of relevant methodological developments in the field of safety suggest that expectations should remain modest regarding the speed of development.

Specific work in FY09 could, *inter alia*, focus at the following: finalizing the proposed SBD process for use by DOE and performing a pilot application on a DOE project currently in the planning phase; developing regulatory options for mandating SBD; further development of safeguards related design guidance, principles and requirements; development of a specific SBD process tailored to the NRC environment; and, pending the completion of the Generic SBD Process, development of an engagement strategy for the IAEA and other international partners.

CONTENTS

FIGURES

TABLES

ACRONYMS

AP	Additional Protocol
CD	Critical Decision
CFR	Code of Federal Regulations
CSA	Comprehensive Safeguards Agreement
DIE	Design Information Examination
DIQ	Design Information Questionnaire
DIV	Design Information Verification
DOE	Department of Energy
EFL	Eligible (Nuclear) Facilities List
IAEA	International Atomic Energy Agency
INCOSE	International Council on Systems Engineering
ISBD	Institutionalizing Safeguards-by-Design
ISSM	Integrated Safeguards and Security Management
MC&A	Material Control and Accountability
MFFF	Mixed Oxide Fuel Fabrication Facility
NGNP	Next Generation Nuclear Plant
NGSI	Next Generation Safeguards Initiative
NNSA	National Nuclear Security Administration
NNWS	Non-Nuclear Weapons States
NPT	The Treaty on the Non-Proliferation of Nuclear Weapons
NRC	Nuclear Regulatory Commission
PR&PP	Proliferation Resistance and Physical Protection
PRD	Program Requirements Document
RRP	Rokkashomura Reprocessing Plant
SBD	Safeguards-by-Design
SLA	State-Level Approach
SSAC	State System of Accounting and Control of Nuclear Materials
SSC	Structures, Systems, and Components
SSSP	Site Safeguards and Security Plan
U.S.	United States (of America)
UCNI	Unclassified Controlled Nuclear Information
VOA	Voluntary Offer Agreement

Institutionalizing Safeguards-by-Design: High-level Framework

1. INTRODUCTION

1.1 Institutionalizing Safeguards-by-Design

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

The overarching goal is the implementation of a new global standard for Safeguards-by-Design (SBD) to support the growth of nuclear power while reducing nuclear security risks. This new standard would formalize the worldwide use of the SBD process. The term "institutionalizing" refers to tailoring the SBD process and obtaining regulatory acceptance of this tailored SBD process within the regimes of cognizant oversight organization(s) (e.g., National Nuclear Security Administration [NNSA], Department of Energy [DOE], Nuclear Regulatory Commission [NRC], and/or International Atomic Energy Agency [IAEA]). Application of SBD in the facility design and construction effort is intended to provide early identification of safeguards requirements, intrinsic features, and design options to optimize design, simplify operation, and minimize life-cycle cost. The SBD process manages interaction between safeguards design and the overall design process to progressively increase definition and analysis at each design phase and is expected to enhance the accuracy of project schedules and budget estimates. SBD has the potential to provide the greatest benefit for innovative designs (i.e., designs for which there is little experience upon which to base the selection of major options [flow-sheet, equipment selection, and layout]) that use a developmental approach. Potential benefits are detailed in Appendix A.

The largest and most complex nuclear fuel cycle facilities may have costs of tens of billions of dollars, be major national efforts, and have a planning, construction, and commissioning period of several decades prior to first operation. The design and construction process for a major nuclear fuel

Excerpt from "The Gas Centrifuge and Nuclear Weapons Proliferation"
(Wood et al., 2008)

Uranium enrichment by centrifugation is the basis for the quick and efficient production of nuclear fuel – or nuclear weapons

"With material controls helping to close the loopholes, the application of safeguards to the overall centrifuge complex becomes important again, with a focus especially on uranium flows in the plant. Existing safeguards do not adequately address many of the strategies for centrifuge misuse. Upgrades directed toward better monitoring of enrichment levels and flows are needed both in and around the plant. New technologies, such as radio frequency identification tags, can automate and facilitate the tracking of UF6 containers. On-line monitors can report throughput and enrichment levels in real time.

It is important that any new measures be put in place quickly because several large-scale facilities are under construction or planned for Iran, Brazil, France, Russia, and the US; it will be far more difficult to retrofit those plants later, given the delicate nature of centrifuges and their propensity for failure during spin-up and spin-down. Those facilities are likely to set a de facto standard for new plants in other countries, so there is now a unique opportunity to define a new baseline for best practices and safeguards by design."

cycle facility is very complex. The SBD sub-process is a relatively modest addition to the overall management process. The SBD process needs to retain simplicity and complement, not hinder, the grand scheme while ensuring effective and efficient identification of safeguards requirements, assessment of draft designs to ensure requirements are met, contribution to overall cost, schedule and risk management, and ensure effective two-way communication with the overall design team and the facility stakeholders, including use of appropriate hold points. The careful selection of SBD sub-process steps is crucial to these aims.

The basic ISBD approach is expected to be applicable, with adaptation, to all nuclear facilities regardless of the regulations or directives governing their design, construction, and startup. Although the regulatory environments differ, the same basic decisions need to be made and the same basic management processes are used. Some regulatory environments mandate additional management controls and approvals beyond the minimum required for efficient project management. However, these additional controls and approvals are not expected to affect the efficacy of the SBD elements proposed.

1.2 Design and Construction Management

1.2.1 Project Management

Most projects requiring major financial commitments, whether carried out by governments or large commercial organizations, are managed using formal project management procedures and processes. There are major professional bodies (e.g., the Project Management Institute) supporting the discipline. In the simplest terms, a project is a unique temporary endeavor with a set beginning and definite end. The Project Management Institute defines project management as “The application of knowledge, skills, tools, and techniques to a broad range of activities in order to meet the requirements of a particular project.” The process of project management is often divided into five types of activities: initiating, planning, executing, monitoring/controlling, and closing. Most large organizations define the high-level project management processes to be used for particular categories of work. These processes generally include policies, directives, manuals, standards, codes, and guides.

In the nuclear industry, the project management process for facility construction is normally supplemented with other regulations and directives specific to disciplines required for project and execution including quality assurance, nuclear and industrial safety, and safeguards and security. Project management for large value projects is generally organized by project phases, which are associated with a logical maturing of broadly stated mission needs into well-defined requirements that can ultimately be translated into the design and construction of a facility that meets customer needs (see Figure 1-1).

1.2.2 Facility Design Process Including Safety

Once the need for a project has been established, the next step is the design process, which translates the mission need into a set of detailed specifications that can be pursued to design and construct the facility. Starting from the project need, the design team develops and evaluates approaches for a facility and processes that meet the need. The feasible approaches are constrained by a set of requirements. Some requirements are derived from the project need itself. Others, such as safeguards and safety requirements, derive from the properties of the materials and processes and the associated regulations, as necessary, to meet the project need. In addition to requirements on the design itself, requirements, such as codes and standards, personnel procedures, safety standards, and quality assurance requirements, are imposed on the design process. The objective of the design team is to develop an optimal approach, in terms of cost and schedule constraints, for meeting all the requirements. The design process is often segmented into phases of increasing definition, detail, and cost in order to minimize project risk and maintain customer involvement. One phased approach is composed of stages for planning, and conceptual, preliminary, and final designs, together with construction. Decision points between each of these phases allow

management to verify that the proposed design meets the complete set of requirements and is feasible (see Figure 1-1). As the design becomes more detailed, it is possible to establish more precise estimates for cost and schedule. Typically, the project team provides the customer with a series of project deliverables at the end of each phase, describing the design, the strategy for meeting various types of requirements (e.g., safeguards and safety), and estimates of project cost, schedule, and risk. Systems engineering (discussed in Section 2.2) provides a structured process and set of tools to aid designers in achieving this objective.

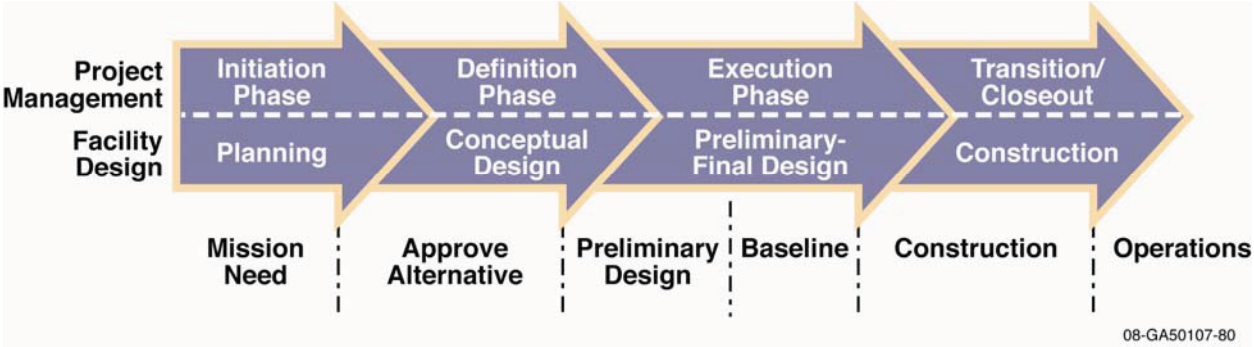


Figure 1-1. Typical phases of project management and design processes.

The design costs associated with each phase increase rapidly from the initiation phase to final design. Conceptual design has often been conducted at the 1 to 10% of total design budget—a wide range, but much smaller cost magnitude than later stages. However, the technical approaches established during conceptual design often commit the majority of project costs (as much as 80% of the total life-cycle costs [INCOSE 2007]). If the fundamentals of the design concept are later found to be incapable of meeting project requirements and are fundamentally changed, then rework or a completely new detailed design may be required with significant cost increases and schedule delays. For first-of-a-kind facilities, such as complex nuclear facilities, engineering costs—mainly design and development—may be in the range 20 to 50% of total project cost to start of operation. If a design concept is found incapable of meeting requirements during the construction phase, the cost and schedule impacts may be much larger because of the possible need for construction rework, new construction, procurement of long-lead time items, and/or increased interest payments. Situations requiring significant design or construction rework have typically arisen because of incomplete understanding of requirements during the earlier design phases or because of the need to accommodate changes to requirements late in the design process. This experience provides a strong incentive to ensure all requirements are well understood and any uncertainties are resolved as early in design as practicable.

Organizations building large complex facilities have attempted to address this problem by front-end loading design work. The front-end loading process includes “pre-engineering” design to the extent of about 20% of the overall budget during the conceptual design phase. Available industry statistics support claims that use of similar front-end loading techniques can result in reductions of between 6 and 23% in total project cost.

1.2.3 Systems Engineering

Systems engineering, which has both technical and management processes, is an interdisciplinary field of engineering that focuses on how complex engineering projects should be designed and managed. The discipline has become an effective way to manage complexity and change. Reducing the risk associated with new systems or modifications to complex systems remains the main objective. The standard ISO/IEC 15288:2002(E)-Systems engineering—system life-cycle processes provides a generic

process description whereas the International Council on Systems Engineering (INCOSE), through the handbook INCOSE-TP-2003-002-03.1, August 2007, elaborates on the processes and activities needed.

The conceptual design phase of a new system may often incur approximately 8% of the life-cycle cost, but at this point the selected conceptual design has committed around 70 to 80% of life-cycle cost (INCOSE 2007). This funding of commitment of an order of magnitude greater cost is broadly known to many areas of the engineering profession and has triggered various responses, including the recent approach of front-end loading. The same logic also applies to the application of an SBD process (as described later in this report), where again the emphasis on early design involvement and definition is all important.

Because systems engineering is the method employed to manage system functions and requirements and project risk, it is important for SBD that the safeguards requirements and the strategies for meeting them be effectively integrated with project systems engineering activities. This integration is fostered by a formal process that mandates development of a design strategy for meeting safeguards requirements; early safeguards categorization of the planned facility; early identification of intrinsic features required or beneficial for meeting safeguards requirements; taking a conservative approach to safeguards requirements and the capabilities of the structures, systems, and components (SSC) to meet these requirements early in design; and use of a structured program to identify and manage project risks associated with meeting safeguards requirements. This is facilitated by an early evaluation of probable security concerns and design basis threat assessment for the planned facility and early participation in the project by the security program representative.

1.3 Project Scope and Structure of the Report

This report describes the results of the seven work scope items for the Project Work Plan for the FY-08 Task: Institutionalizing Safeguards-by-Design, Task I.D. 24.243.2.6.9, Rev. 6: 01-26-08, see Appendix B, which includes:

A. High-level framework for Institutionalizing Safeguards-by-Design

B. Identification and description of requirements and methodology

C. Optioneering study—Design and construction management with SBD process for DOE domestic regulatory environment including international Safeguards

D. Best practices and lessons learned review

E. Working with the IAEA

F. Summary and path forward – Institutionalizing Safeguards-by-Design

G. Support Advanced Fuel Cycle Facility (AFCF) Design Project.

An important recent application of safeguards design processes in the U.S. national context arose within the conceptual phase of facility design, as sponsored by DOE, Office of Nuclear Energy, for the AFCF, an engineering development test bed. This set the first direction of work in this report to developing SBD within the DOE oversight environment. The ISBD project approached this effort by selecting the design, construction, and startup of a U.S. DOE nuclear facility as the study and baseline for use in the development of the process for SBD. The DOE design and construction process, which is representative of nuclear facility design and construction activities, is prescribed in considerable detail within the DOE directive system. The directive system provides a well-defined baseline to which specific SBD elements can be added. The DOE directive system includes requirements for integration of safety into design (see Appendix I) and initial guidance for integration of domestic security into design. This preexisting infrastructure helped the team select methodology and pinpoint areas where SBD elements

could be effectively added to the design and construction process and expedited the development of both the high-level framework and some of the implementation details.

The SBD team examined design processes, best practices and lessons learned from major design projects, and developments in nuclear safety, and project and systems engineering, in order to conceptualize the framework of essential elements for SBD. The SBD framework consists of three pillars (requirements definition, design processes, and technology and methodology) standing on the foundation of institutionalization and needed to support the achievement of a global SBD standard (see Figure 1-2). The focus of the work in FY-08 was on SBD processes for design, but all the areas contributed to defining work needed for the future. Although creation and testing of the SBD process within the various oversight environments are important activities under the ISBD framework, many other activities are essential to meet the ultimate goal. The ISBD high-level framework includes the diverse activities needed to institutionalize SBD including consulting tasks, technical tasks, establishing directives and guidelines, pilot testing, international support, supporting commercial projects, holding workshops, promotional activities, and many others. During the FY-08 project, two additional work areas—the NRC regulatory environment and formulation of a generic SBD process—became important.

Figure 1-2. Categorization under high-level framework.

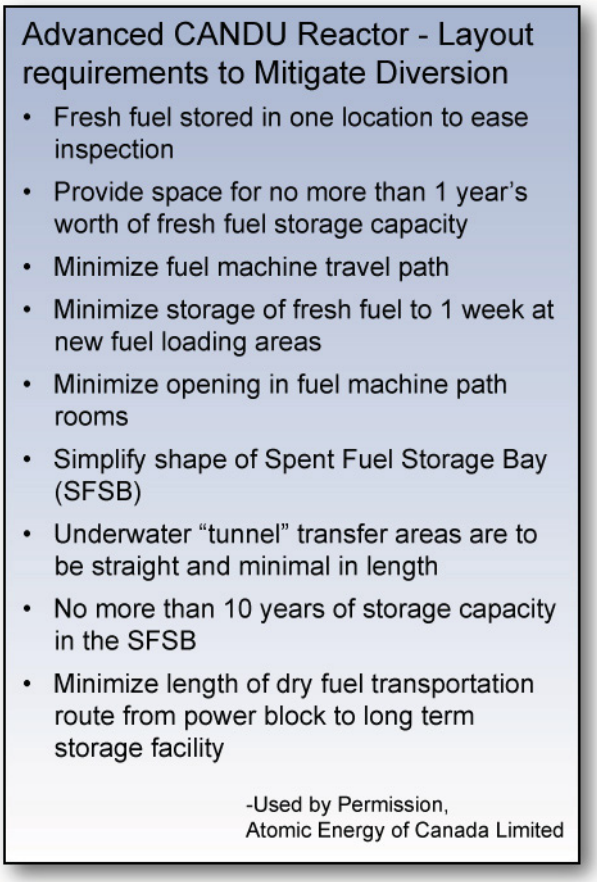
The structure of the report follows Figure 1-2. Sections 2 through 5, respectively, cover requirements definition, design processes (including SBD), technology and methodology, and institutionalization. Section 2 outlines prescriptive, mainly regulatory, and performance requirements. In Section 3, studies on the design and construction process in the DOE environment with integration of SBD for domestic regulatory requirements and international safeguards are reported. A range of technical solutions are discussed in Section 4 including a holistic assessment of safeguardability, proliferation resistance, technical difficulty, and cost efficiency because these areas remain controversial for the application of analytical methods. Section 4 also presents various best practices, lessons learned, and current NNSA and IAEA developments. The proposed institutionalization approach is presented in Section 5, which describes progress in FY-08 and future work options under the high-level framework. Section 6 presents a generic SBD process integrated with a generic design process and derived from the team members' capabilities and recent experience with the example of SBD in the DOE environment. It illustrates the essence of the SBD process, has potential for wide international application, and has value as a training aid. Section 7 presents the conclusions and recommended path forward. Sections 8 and 9 provide a list of references and the glossary, respectively.

Volume 2 contains a set of 12 appendixes that provide additional material describing:

A. Potential benefits of SBD
B. ISBD project work plan
C. Evolving approach to nuclear safety
D. National and international safeguards requirements for the nuclear fuel cycle
E. Flowcharts of SBD process for DOE domestic regulatory environment
F. IAEA process for international safeguards
G. Flowcharts of SBD process for DOE domestic regulatory environment with international safeguards
H. Applying best practices and lessons learned to ISBD
I. Guiding principles for safety-in-design
J. Outline for possible DOE directive on SBD
K. Survey of NRC arena for application of SBD
L. Volume 2 References

2. SAFEGUARDS REQUIREMENTS FOR DOE DESIGN AND CONSTRUCTION MANAGEMENT

Requirements drive project execution. This section provides requirements for the SBD process and for domestic and international safeguards. Confirmed methodologies are needed to decide whether requirements are met by proposed designs. All requirements necessary for the successful execution of SBD must be formalized so that they are accounted for within the project structure. All required work shall be completed, and all work performed should be required. A full assessment of conceptual design to confirm that it meets all requirements is essential prior to initiating later design phases. The same applies for the more detailed examination of design adequacy in fulfilling the later, more detailed, and comprehensive system descriptions and component specifications before initiating fabrication, etc.



Project requirements often fall into two categories. The first is composed of those attributes that the project is expected to demonstrate once it is completed. For a nuclear facility, performance requirements (internal requirements) may include parameters such as storage capacity, production rates, availability, product properties, and other items that are adjunct to the mission but are of major importance such as safety and security. The second category is composed of prescriptive requirements (external constraints) that deal with project delivery (i.e., nuclear facilities must comply with regulatory directives and standards for quality assurance in design and construction of the nuclear fuel cycle). Other prescriptive requirements include calculation methods, reports and data to be developed and submitted at specific stages, approvals that must be received, codes and standards to meet, and mandatory reviews. Requirements for development of the generic SBD process itself, are those for a new design procedure as opposed to a new facility. So, perhaps unsurprisingly, the high-level requirements for the SBD process include regulatory aspects in both performance and prescriptive requirement areas.

The first purpose of this section is to identify the high-level requirements pertaining to the SBD process (i.e., performance-related requirements) within the context of a modern project for which proliferation risk reduction and international safeguards are also to be applied. These high-level requirements for the SBD process are mainly qualitative, at present, and concern its effectiveness, robustness, and flexibility for safeguards design. They have not been derived from first principles (e.g., formalized through the Integrated Safeguards and Security Management [ISSM] framework [DOE P 470.1, 2001] in the DOE system), nor validated through trade studies (INCOSE 2007). Such studies are suggested for the future and this report is expected to be a valuable aid. Lower-level requirements, such as specifications for performing particular safeguards assessments, are likely be considerably more definitive and prescriptive. Secondly, current safeguards directives (i.e., prescriptive requirements) for the nuclear fuel cycle must be taken account of and are described in greater detail in Appendix D. Any new directives needed will be consistent with, enhance, or supersede existing ones. The

combination of proliferation risk reduction, including international safeguards, together with national considerations has not routinely been applied within a Nuclear Weapons State. This is a significant change for a U.S. project. Requirements for application in an arbitrary foreign country were not to be considered under the scope of FY-08 work. Interactions with (U.S.) state and local institutions will also need to be examined in the future.

2.1 Performance Requirements for the SBD Process

The objective for the SBD process is to provide a procedure by which international and national safeguards, physical security, and other nonproliferation objectives are fully integrated into the overall design and construction process for a nuclear facility, from initial planning through design, construction and operation, with the goal of increasing the safeguardability of facilities. Although elements of SBD are incorporated in each phase of the project management process, the focus is on the early phases, consistent with the front-end loading concept discussed in Section 1.2. The generalized SBD elements for each phase of a project are described in the list that follows.

The high-level requirements, formulated by the SBD team, are:

1. Develop a simple, concise, formalized, and integrated process for SBD that is acceptable to stakeholders.
2. Develop the SBD process to be compatible with and enhance the structure and methodology of the applicable directives and standards, as far as they are known, as well as known future direction. This includes NRC, IAEA, and DOE requirements for those projects to which such requirements apply.
3. Base the SBD process on accepted project management, design, and systems engineering processes.
4. Provide an SBD approach that is flexible and suited to deployment in a variety of regulatory contexts.
5. Supply a useful tool for the project manager responsible for the design, construction, and startup of nuclear facilities.
6. Identify and mandate a minimal but complete set of deliverables for safeguards design to provide systematic, comprehensive, auditable, and transparent input to the project management, design, and systems engineering processes.
7. Provide progressive and phased development of safeguards effectiveness reports to support design and to seek active dialog with and agreement by the sponsor as demonstrated by their provision of phased acceptance reports.
8. Initiate safeguards design activities in the preconceptual planning phase of the design process so that the impact of safeguards requirements on facility alternatives analysis will be effectively evaluated during the conceptual design phase.
9. Treatment of nuclear security will contribute fully to the design process including meeting all relevant design requirements.
10. Mandate the early appointment of a safeguards team leader and the subsequent creation of the safeguards design team with clearly defined roles and responsibilities.
11. Use systems engineering processes to develop the optimum integration of operation, safety, safeguardability, protectability, and proliferation resistance into the facility design.
12. Provide early identification of intrinsic design features that enhance safeguards, security, or proliferation barriers, or that facilitate the implementation of extrinsic safeguards, security, or nonproliferation measures.

13. Mandate the use of life-cycle cost analysis as a key criterion for capital expenditure decisions between intrinsic (early) and extrinsic (later) design alternatives.
14. Provide safeguards, security, and proliferation mitigation throughout the facility at minimum capability consistent with regulatory and other requirements while minimizing the life-cycle costs to the operator and regulatory agencies.
15. Identify and incorporate the key integration activities necessary to efficiently incorporate IAEA safeguards into the design of nuclear facilities.

2.2 Areas of Prescriptive Requirements for Safeguards

The SBD process must comply with current safeguards concepts, agreements, directives, etc. for the nuclear fuel cycle. Of course, the nuclear fuel cycle facility itself, as designed, constructed, commissioned, operated, and decommissioned must also comply with these requirements as well as many others. The main national and international requirements affecting safeguards are detailed in Appendix D. Various high-level prescriptive requirement areas are as follows:

1. National Safeguards. "A nation's integrated 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." (extension from DOE M 470.4-7, 2005) For the United States, DOE directives, NRC regulations, and Codes of Federal Regulations (CFRs) are predominant for federal and commercial sectors; although in some cases, NRC delegates regulatory authority for various facilities to the state level.
2. Physical Protection. "The application of physical or technical methods designed to protect personnel; prevent or detect unauthorized access to facilities, material, and documents; protect against espionage, sabotage, damage, and theft; and respond to any such acts should they occur" (DOE M 470.4-7, 2005). A number of policies and procedures are in place domestically to cover physical protection requirements at DOE sites. In November 2007, DOE issued a new guide to ensure that safeguards and security requirements are identified and integrated into a project early and that their implementation is assessed throughout the project life cycle.
3. Material Control and Accountability (MC&A). "Those parts of the safeguards program designed to provide information on, control of, and assurance of the presence of nuclear materials, including those systems necessary to establish and track nuclear material inventories, control access to and detect loss or diversion of nuclear material, and ensure the integrity of those systems and measures." (DOE M 470.4-7, 2005) DOE, NRC, and IAEA requirements quantify the criteria regarding protracted and abrupt diversion, as wells as describing the inventory taking requirements.
4. International Safeguards. "Under the Treaty on the Non-Proliferation of Nuclear Weapons (Nuclear Non-Proliferation Treaty [NPT]), the verification measures applied by the IAEA to detect the diversion of nuclear material in a timely manner from peaceful uses to nuclear weapons or other nuclear explosive devices." (DOE M 470.4-7, 2005) Regarding international safeguards, the detection of undeclared nuclear materials and activities is often considered the greatest contemporary challenge. IAEA expresses this as the need for international safeguards to provide assurance of the completeness of a state's declaration as well as its correctness for the activities declared. The IAEA Safeguards Glossary (2001 Edition) provides a valuable source document for reaching IAEA legal instruments and other IAEA safeguards documents.

Several other areas are being studied by Generation IV International Forum (GIF) and IAEA International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO). Whilst these have not been accepted internationally in terms of requirements or methodologies for assessing designs, studies are progressing.

1. Proliferation Resistance (PR; Gen IV). “Is that characteristic of a nuclear energy system that impedes the diversion or undeclared production of nuclear material or misuse of technology by the host state seeking to acquire nuclear weapons or other nuclear explosive devices.” (Gen IV, PRPPWG/2006/005 Rev. 5) Intrinsic proliferation resistance features are those that result from the technical design of nuclear energy systems, including those supporting implementation of extrinsic measures. Extrinsic proliferation resistance measures are those resulting from states’ decisions and undertakings relevant to nuclear energy systems. A measure of one important aspect of proliferation resistance is that of “safeguardability.”
2. Safeguardability. “The degree of ease with which a system can be effectively and efficiently put under international Safeguards.” (Gen IV, PRPPWG/2006/005 Rev. 5) This definition covers both intrinsic and extrinsic features. Proliferation resistance measures are barriers against a national adversary illicitly acquiring nuclear weapons through diversion from or misuse of infrastructure for nuclear energy systems. There are no formal requirements that proliferation resistance must be considered although the Generation IV Proliferation Resistance and Physical Protection (PR&PP) methodology and the IAEA INPRO study support this principle, see Section 4.

2.3 Prescriptive Requirements from DOE Environment

DOE employs a comprehensive set of directives (www.directives.doe.gov/), including those for the design and construction process, i.e., Acquisition of Capital Assets, which covers nuclear facilities. The DOE acquisition directives include the number 413 series of policies, orders, manuals, and guides. The acquisition management directives are supplemented by many other regulations, directives, and standards specific to disciplines required for project management and execution, including quality assurance, nuclear and industrial safety, and safeguards and security (see Tables 2-1 and 2-2).

The DOE Acquisition Management System is organized by project phases and Critical Decisions (CD), which represent a logical maturing of broadly stated needs into well-defined requirements that can ultimately be translated into a facility that meets a DOE mission need. Figure 2-1 illustrates a typical implementation of the DOE Acquisition Management System for Line Item Projects (DOE O 413.3A, 2006).

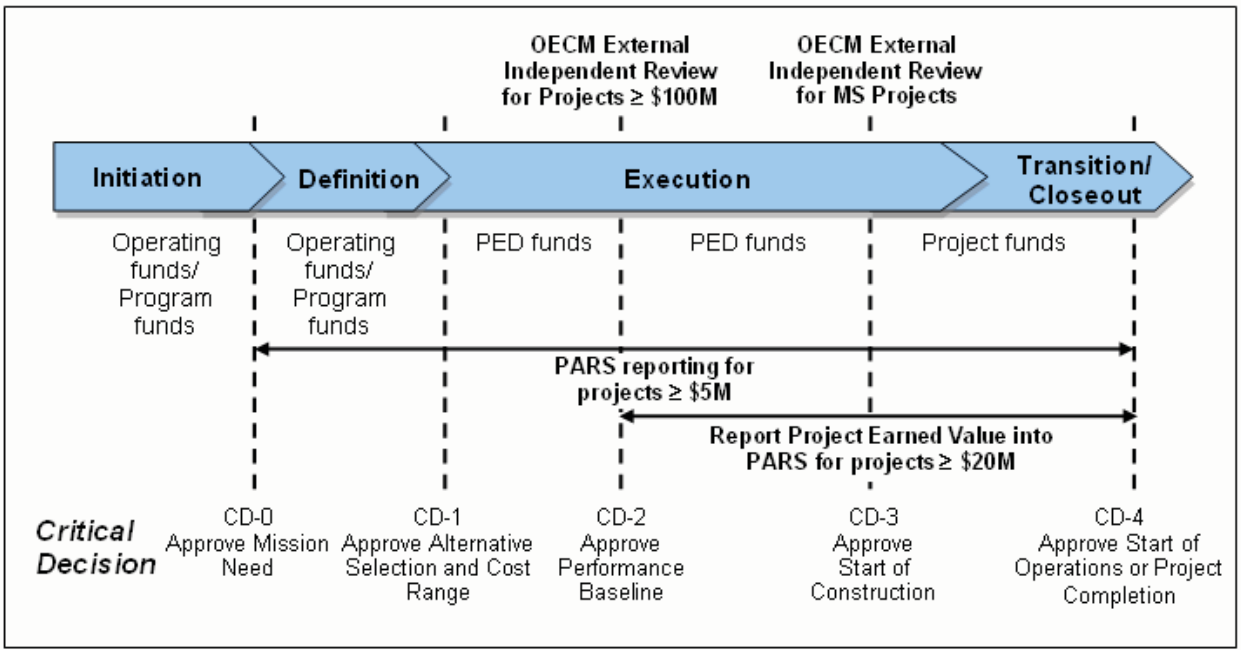


Figure 2-1. Typical DOE Acquisition Management System for line item projects (DOE O 413.3A, 2006). (OECM = Office of Engineering & Construction Management, PARS = Project Assessment and Reporting System)

The DOE Order 413.3A, 2006, calls out other relevant DOE directives and a number of these are shown in Table 2-1.

Table 2-1. Selected DOE directives for nonproliferation, safeguards, security, and safety that are mainly called out by DOE acquisition management directives, e.g. DOE O 413.3A, 2006.

Subject	Directive
Safeguards with IAEA	DOE O 142.2A
National Security, Cyber Security, etc.	DOE P 205.1, O 205.1A, M 205.1-3, M 205.1-4
Safeguards & Security Implementation	DOE G 226.1-1
Nuclear Safety	DOE P 410.1A, O 410.1, 10 CFR 830
Acquisition Management	DOE P 413.1, O 413.1A, O 413.3A, M 413.3-1, G 413.3-3
Facility Safety	DOE O 420.1B, G 420.1-1
Integrated Safeguards and Security Management	DOE P 470.1, O 470.2B, O 470.3A, O 470.4A, M 470.4-1 Chg 1, M 470.4-2 Chg 1, M 470.4-3 Chg 1, M 470.4-4 Chg 1, M 470.4-5, M 470.4-6 Chg 1, M 470.4-7
Nuclear Materials Management	DOE O 5660.1B
Control and Accountability of Nuclear Materials	DOE 5633.2A, DOE 5633.3A, DOE 5633.4, DOE 5633.5 DOE 5635.1A
Radioactive Waste Management	DOE 5820.2A
Integration of Safety into Design	DOE-STD-1189-2008

Directives dealing with integrated safeguards and security (includes physical protection) and nuclear material control and accountancy (DOE MC&A) are particularly relevant to the overall safeguards area. Purely as an example, the set of principal directives for physical security, one of the high-level prescriptive requirement areas called out by the DOE Acquisition Management System, is provided in Table 2-2. Many other relevant prescriptive requirements are summarized in Appendix D.

Table 2-2. Selected prescriptive requirements relating to physical protection.

No.	Title
DOE O 413.3A	Program and Project Management for the Acquisition of Capital Assets
DOE G 413.3-3	Safeguards and Security for Program and Project Management
DOE M 461.1-1	Packaging and Transfer of Materials of National Security Interest Manual
DOE O 461.1A	Packaging & Transfer or Transportation of Materials of National Security Interest
DOE P 470.1	Integrated Safeguards and Security Management Policy
DOE O 470.2B	Independent Oversight and Performance Assurance Program
DOE O 470.3A	Design Basis Threat Policy
DOE M 470.4-1	Safeguards and Security Program Planning and Management
DOE M 470.4-2	Physical Protection
DOE M 470.4-2	Safeguards and Security Alarm Management and Control Systems
DOE M 470.4-3	Protective Force
DOE M 470.4-4	Information Security
DOE M 470.4-5	Personnel Security
DOE M 470.4-7	Safeguards and Security Program references
DOE O 470.4A	Safeguards and Security Program

DOE NNSA requires the submission of a Program Requirements Document (PRD) for construction programs/projects being executed by NNSA (NNSA Policy Letter BOP 50.004, 02 15 2008). This instrument may be a very convenient vehicle to implement new requirements for NNSA projects.

2.4 Prescriptive Requirements from International Safeguards

2.4.1 Summary of IAEA-USA Safeguards Environment

Countries that are a party to the Treaty on the Non-proliferation of Nuclear Weapons are obliged to conclude a safeguards agreement with the IAEA to safeguard nuclear material within the country and ensure that it is used for peaceful purposes. This safeguards agreement typically follows the IAEA INFCIRC model (IAEA INFCIRC/153 [corrected] 1972). The agreement establishes requirements for countries and the builder/operators of nuclear facilities that impact the design, startup, and operation of the facilities. This is the case even for some nuclear weapons states, which have acceded to the voluntary offer agreement (VOA), excluding only those facilities with direct national security significance. Recently, many states have or are in the process of acceding to Additional Protocols (APs), which provide IAEA with a much fuller range of safeguards measures at its disposal to specifically target undeclared activities and facilities. The new safeguards regime is based on a state-level approach (SLA) that considers acquisition paths specific to each state. Nondiscriminatory criteria have been established for the process of defining the SLA tailored to the assessed situation for each state. New techniques and broader approaches to verification are being adopted. Emphasis is being shifted away from routine inspections to expert judgment and “unpredictable inspections,” i.e., very short notice inspections and verification

activities. All inspection activities are concerned with the potential existence of undeclared nuclear material and activities. These new processes, called "integrated safeguards," increase both efficiency and effectiveness and are based on the individual SLA. The objective of IAEA integrated safeguards is to make an optimal set of safeguards measures available to the IAEA for verification of each state's declaration under the terms of the Comprehensive Safeguards Agreement (CSA) and AP (IAEA—Carlson 2006).

The high-level structure of U.S. obligations, federal regulations and facility design interfaces with IAEA agreements under the NPT, are shown in Figure 2-2. The boxes under "International Oversight" summarize high-level steps during facility design, construction, and operation.

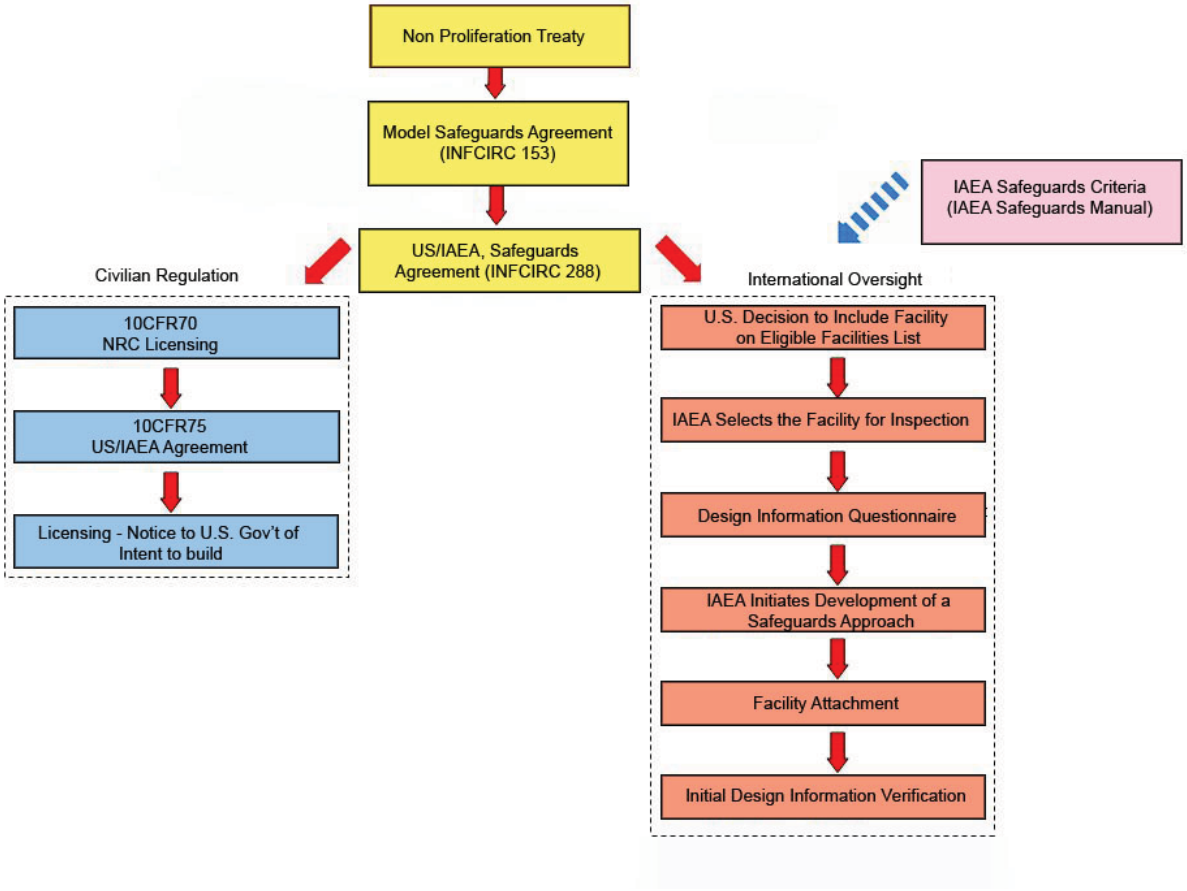


Figure 2-2. Structure of U.S. obligations, regulations, and interfaces with IAEA.

DOE offers access to IAEA to carry out inspections of DOE facilities listed under the eligible (nuclear) facilities list (EFL). The DOE Order 142.2A, December 2006 (Voluntary Offer Safeguards Agreement and AP with the IAEA) – NNSA, and the DOE Manual 142.2-1, September 2008 (Implementation of VOA and AP with IAEA) – NNSA are the relevant directives. DOE also has an AP Web Site (https://www.ap.doe.gov), which contains information and tools to assist Headquarters, field elements, and contractors in implementing the AP. The site allows for secure access to AP-related documents, frequently asked questions, links to other AP-related web sites, computer-based AP training modules, etc.

The EFL for the U.S. includes all commercial facilities regulated under the NRC and most facilities controlled and regulated by DOE that handle nuclear material. The current list contains approximately

265 facilities, of which approximately 240 are NRC licensees. Annually, the IAEA Safeguards Department randomly selects facilities from the EFL for inspection. For the U.S., around five different facilities per year are selected for routine inspection, and these are often rotated the following year. However, any facility on the EFL may be selected for safeguards inspection, and so it must be possible to apply IAEA safeguards and meet IAEA safeguards objectives. This is a key reason why the SBD process must be able to cover international safeguards, and nuclear facility designers are aware that, even in nuclear weapons states including the U.S., all eligible facilities need to be able to meet IAEA safeguards requirements.

The U.S. AP was signed by the United States Government in 1998, and the U.S. Senate subsequently provided its consent to ratification as a treaty on March 31, 2004. The U.S. Congress passed and the President signed the U.S. Additional Protocol Implementation Act on December 16, 2006. Next, the President issued Executive Order 13458 on February 4, 2008, authorizing the Executive Branch agencies to mandate regulations. The U.S. Additional Protocol will enter into force after the federal agencies have promulgated regulations and completed all implementation. Interagency procedures, which are periodically issued by the Department of State, implement the AP. When the AP enters into force, all U.S. programs will be subject to strengthened reporting requirements and expanded IAEA access rights.

2.4.2 IAEA Requirements during Facility Design, Construction, and Operation

This section summarizes the IAEA safeguards requirements during the expected many decades of facility design, construction, commissioning, and operation—see Appendix F for a more detailed account of this information. All countries that intend to build nuclear facilities will officially notify the IAEA, as soon as the decision is made by national authorities to construct, or license the construction of facilities, i.e., the national authority must notify the IAEA before construction begins. In nuclear weapons states and for example in the U.S., inclusion in the EFL is interpreted by the IAEA as official notification of the construction of the facility.

IAEA/JAEA Workshop – Tokai-mura, Japan, November, 2007

Advanced Safeguards Approaches for New Reprocessing Facilities (Durst, 2007)

- Project sponsored by U.S. NNSA, Office of NA-243
- Study identifies “development needs” for technologies and methods to safeguard future reprocessing plants
- It may be possible to reduce batch verification frequency if “Process Monitoring” is developed
- An effective Safeguards Approach for the aqueous line at AFCF can be developed, based on the approach at RRP
- It will be very challenging to meet the IAEA inspection goals for a 3,000 tonne per year plant (CFTC)
- It would be easier to meet these goals if the plant were constructed of four 700 to 800 t/year process lines

Clear need for early Safeguards involvement in facility design due to potential severe economic impact of multi-line process

The four main elements of the IAEA process to develop and apply a facility-specific safeguards approach are:

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

The safeguards agreement gives requirements for the submission, evaluation, and verification of safeguards relevant facility design information by

the state to the IAEA. This design information is provided in a standardized questionnaire and form called an IAEA DIQ. The DIQ provides the IAEA with enough information to evaluate the operator's declaration for the nuclear facility to be constructed, especially regarding its function, capacity, process employed, nuclear materials, waste, and mode of operation. More detailed information required on nuclear materials includes: amounts (by element and fissile isotope), measurement and inventory procedures, flow paths inside and outside the facility, type and capacity of transfer containers, and waste processes and procedures for assaying waste containers.

After submitting the initial DIQ, the national authorities, facility operator, and the IAEA begin discussing and negotiating the "Subsidiary Arrangements" (to the safeguards agreement), relevant to the facility being constructed. The Subsidiary Arrangements consist of a General Part, applicable to all common nuclear activities of the country, and a "Facility Attachment," prepared for each facility in the country and describing safeguards arrangements specific for that facility. The Facility Attachment describes in detail what inspection activities will be performed in the facility, the instruments to be used (both operator and inspector), the frequency of inspections, and estimated level of inspection effort. Because these are facility specific, they must be negotiated while the facility is being designed and constructed. Even though the national authorities and builder/operator of the nuclear facility have significant input into the Facility Attachment, the IAEA must approve it, because it will dictate whether IAEA safeguards can, or cannot, be practically implemented at the specific facility. The Facility Attachment evolves during the design, construction, and testing of the facility. In principle, it captures the facility-specific issues relevant to safeguarding the facility and implementing the IAEA's "Safeguards Approach" described later.

After the facility operator or designer/constructor has prepared the IAEA DIQ and submitted it to the national nuclear authorities for forwarding to the IAEA, the IAEA will start reviewing the information and schedule follow-up DIV activities. The purpose of the DIV is for the IAEA to confirm that the advance declarations regarding the type, size, and purpose for the new nuclear facility are correct and complete. If safeguards relevant information has not been fully provided, then the IAEA will request additional clarification, and information. In performing the DIV, IAEA safeguards inspectors will survey the site from the earliest stages of construction to confirm the location and size of the facility and to determine that the incipient construction is consistent with that facility type. The process of examining the facility design information is called the Design Information Examination (DIE). These activities continue over the whole life cycle of the facility. During facility construction, the IAEA continues DIE at the facility site during the excavation of the main structures and construction of the facility and performs initial DIV activities, confirming the building size and profile, paying close attention to the possibility of undeclared sub-basements, pipe chases, and other interconnections with ancillary structures on site. Building dimensions are measured, layouts confirmed, and an initial survey for the placement of safeguards-specific instruments and systems made. The emphasis during this stage is on confirming that the facility being constructed is consistent with the type, size, and purpose of the nuclear facility as conveyed by the national regulatory authorities in the DIQ.

The IAEA "Safeguards Approach" describes the specific safeguards verification and accountancy measures that will be implemented at the facility to meet the IAEA safeguards inspection goal. The goal is to detect, with a high level of confidence, the diversion of one "Significant Quantity" of safeguarded nuclear material within a period for timely detection. The Safeguards Approach is prepared and approved exclusively by the IAEA. It is not an external document, nor is it approved by the national authorities. However, the Safeguards Approach depends on the Facility Attachment, which does permit the national authorities and facility builder/operator an opportunity for ensuring that the Safeguards Approach will not be excessively burdensome and inefficient, or inappropriate for the facility being constructed. The Safeguards Approach is based on the "Safeguards Criteria" and requirements noted in the IAEA Safeguards Manual. However, the IAEA may customize the safeguards approach for implementing safeguards on a site or state level, depending on the circumstances for the particular country. What is

relevant to this discussion is that the Safeguards Approach should be completed and approved by the IAEA before the facility operates—although the onus for this is more upon the IAEA than the national authorities or facility builder/operator.

Under the comprehensive (INFIRC/153-type) safeguards agreement, more detailed IAEA requirements include that nuclear facilities will have, use, or permit:

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

Safeguards inspection requirements 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. These criteria specify the facility safeguards requirements additional to those in the Safeguards Agreement. The safeguards requirements depend on the type of nuclear material, whether irradiated or unirradiated, and closeness to direct use to produce a nuclear weapon.

For each type of nuclear facility, the Safeguards Criteria specify requirements for:

Examination of safeguards relevant operating records and state reports

Performance of annual Physical Inventory Taking and Verification

Verification of domestic and international transfers of nuclear material

Verification of other nuclear inventory changes

Verification of nuclear material flow at "Other Strategic Points"

Confirmation of nonproduction of Direct Use Material

Confirmation of the absence of borrowing of nuclear material between facilities or Material Balance Areas

Performance of nuclear Material Balance Evaluation

Verification activities at Interim Inspections for timely detection of diversion

Verification of and follow-up for safeguards "Discrepancies" or "Anomalies"

Verification of facility "Design Information"

Verification of the facility operator's measurement systems (used for safeguards)

Confirmation of nuclear material transfers

Verification activities related to partial attainment of IAEA inspection goals

Verification related to non-nuclear material under safeguards (e.g., heavy water)

Verification activities related to equipment and facilities under safeguards

Activities for the preparation of inventories of nuclear material, equipment, and facilities.

These facility-specific requirements 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, providing minimal but adequate facilities and minimizing impact on operational procedures and costs. For this reason, an improved approach should be considered that encourages earlier and more complete interaction and collaboration between the facility designers, State System of Accounting and Controls (SSAC), and the IAEA.

3. DOE DESIGN AND CONSTRUCTION MANAGEMENT WITH SAFEGUARDS-BY-DESIGN PROCESS

3.1 Safeguards-by-Design Process in DOE Directives Environment

Section 3 provides the results of an optioneering study, using several multi-day sessions, to develop the SBD process within the:

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

To progress the study, the application of SBD within a particular regulatory system was needed and the DOE environment was selected for the initial study due to the earlier use within the AFCF conceptual design and the completeness and detail of the DOE directive system. The study generated a single process covering DOE domestic regulatory requirements and international (IAEA) safeguards. However, the study was performed in two stages: first, developing a process using DOE domestic requirements and SBD team's performance requirements only (see Section 3.2) and, second, modifying the first results to integrate the additional effects of incorporating international (IAEA) requirements (see Section 3.3). The step-wise approach was to simplify the study and facilitate its visual representation by means of two series of flowcharts, see Appendixes E (domestic environment) and G (domestic environment and international safeguards).

This tests the adaptability and assessed effectiveness of the SBD process in an appropriate environment. The methodology used is also relevant to the tailoring of the SBD process to other environments such as that for commercial facilities regulated by NRC.

3.2 Design and Construction Management with SBD Process for Domestic DOE Safeguards Directives

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

The Program and Project Management group operates as a guiding body that provides leadership for the entire project. The Project Engineering group uses the leadership or guidance from the Program and Project Management group and further specifies or facilitates the execution of the project by interacting

with the SBD team. Actions are performed by the SBD team, and interactions occur with the other teams for Project Engineering, and Program and Project Management. Not only are these interactions shown but also the resulting actions. Some requirements and deliverables forming the SBD process are described below and also are detailed in five flowcharts in Appendix E. The SBD process using DOE domestic safeguards requirements made use of methodology and flowcharts developed for Safety-in-Design as described in the recently issued DOE Standard, DOE-STD-1189-2008. The following description of the SBD process starts before CD-0 and finishes after CD-4.

3.2.1 Project Initiation/Preconceptual Planning

During the initiation phase of the project, the SBD process adds the specific requirement for safeguards categorization of the planned facility and the development of a document that describes how the SBD approach will be tailored to the planned project. The safeguards categorization of the planned facility includes the evaluation of probable security concerns and design basis threat assessment recommended in DOE G 413.3-3. The tailoring strategy describes the projects consideration of the SBD principles, key concepts, and approach in the governing standard, permitting the project manager to identify those aspects of the overall SBD process that are expected to be beneficial for the project and to modify or eliminate those that would not be cost effective if implemented without tailoring. The tailoring also permits more safeguards efforts to be focused on those facilities that pose the greatest international and national safeguards, physical security, and proliferation risk.

A Program Requirements Document (PRD) is submitted for construction programs/projects being executed by NNSA to translate the "need" in the Mission Need Statement into initial top-level requirements addressing such concerns as performance, supportability, physical and functional integration, human integration, security, test and evaluation, implementation and transition, quality assurance, and configuration management.

The SBD process mandates the appointment of an SBD team leader to accomplish these tasks. This individual could be the security program representative identified in DOE-G-413.3-3 or a member of the project team. During this phase, the SBD process also provides for customer (i.e., DOE) approval of the SBD tailoring strategy so that both the project manager and the customer are in agreement about the manner in which the SBD process is to be applied. The customer responds to the SBD tailoring strategy with a report describing its expectations for SBD. The DOE expectations for SBD describe the requirements and approach that DOE expects the project to employ in integrating safeguards into the project commensurate with the information available about targets, potential vulnerabilities, and candidate safeguards measures. This document also records the DOE review of the tailored application of SBD principles, key concepts, and approaches proposed in the tailoring strategy. The customer approval of the SBD tailoring strategy and exposition of its expectations for SBD are part of the package submitted for project CD-0 approval.

3.2.2 Definition/Conceptual Design Phase (CD-0–CD-1)

During conceptual design, the SBD process adds the formation of an SBD team to assist the SBD team lead. The SBD team takes input from the Project Functions and Operational Requirements, which are based on higher level requirements, and they are input into the SBD Conceptual Phase Activities, which form an iterative graded process called the SBD design loop, expressed in Figure 3-1. This loop is also used in later design phases. The internal design steps may be invoked or deferred as the design demands and matures. The design that is passed to the SBD team is modified and reviewed internally until the team is satisfied that it meets the established requirements. At that time, the design will exit the SBD Design Loop to enter a Project Design Review process, conducted by project peers, primarily directed at ensuring that the safeguards design is in alignment with the overall project design. If comments are generated in this review process, the safeguards design is returned to the SBD Design Loop

for resolution of those comments. When the SBD team has resolved these comments to their satisfaction the Project Design Review process begins anew. Throughout this process, interaction with the Project Design (i.e., the other design teams, especially safety) is vital, so that the outcome is mutually acceptable. DOE O 413.3A requires that a contractor's project management system must "at a minimum conduct a Preliminary and Final Design Review, in accordance with the Project Execution Plan. For nuclear projects, the design review will include a focus on safety and security systems."

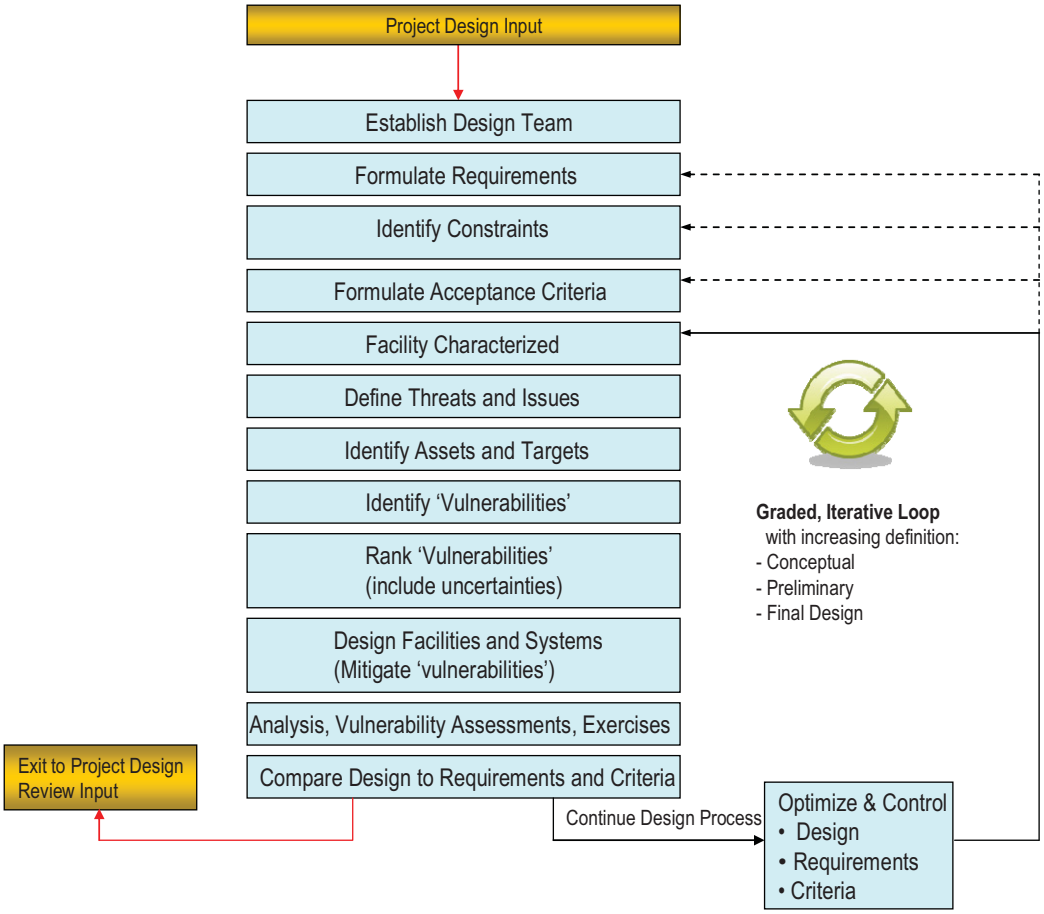


Figure 3-1. SBD design loop.

The preparation of two safeguards documents is currently required by DOE during conceptual design —the vulnerability assessment report and the initial cyber security plan. The SBD team augments the original SBD tailoring strategy to develop an overall safeguards design strategy. The SBD process also mandates two additional analyses to support the early identification of the design features relied on to meet safeguards performance requirements. One of the analyses is the MC&A Process Analysis, which 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 to be tailored to the complexity of the facility and the safeguards significance of the nuclear material housed at the facility. The second analysis is the proliferation barrier/safeguardability analysis, which identifies the design features and associated performance requirements needed to meet intrinsic and extrinsic proliferation resistance requirements. The technical approach for this analysis is discussed in more detail in Section 4.2, "Proliferation Resistance and Safeguardability." Concurrent with the performance of these four analyses, the SBD team augments the SBD tailoring approach discussion of the SBD requirements to

develop a safeguards design strategy. This strategy identifies the design approaches that the project proposes to meet the safeguards requirements from the DOE directives and performance requirements from vulnerability assessment, MC&A process analysis, proliferation barrier analysis, and cybersecurity planning. The latter is an existing DOE requirement that is included here because of its increasingly close relationship to safeguards and security that is evolving toward increased use of integrated, computer-based systems.

The SBD team summarizes the requirements from these four analyses, which may be classified, and the design requirements in the applicable DOE directives in an unclassified (but probably Uncontrolled Classified Nuclear Information [UCNI]) document referred to as the Safeguards Design Functions and Specifications. This document provides the complete set of safeguards requirements, as they are established during this phase, for input to the facility Functional & Operational Requirements document and for use in systems engineering analyses. The collection of these requirements in an unclassified summary makes it possible to provide them to design team members without security clearances, who will need to implement them. It also makes it possible for the security requirements to be considered within the set managed by automated systems engineering and requirements management tools, with the use of computers approved for classified processing. Based on analysis of these requirements and the conceptual design work, the SBD team identifies and describes any areas where new or unproven technology or design approaches are planned to meet the applicable safeguards requirements. Working with the project risk management team, the SBD team evaluates the project risks (e.g., schedule delays, cost increases) associated with each of these unproven systems or design approaches and develops measures to mitigate these (e.g., by use of technology development efforts. This analysis is documented in a safeguards design risk and opportunity assessment for review by the customer's safeguards organization to verify the completeness of the set of identified risks, the feasibility of the proposed risk mitigation measures, and reasonableness of the risk estimates. When a project risk cannot be mitigated to an acceptable level by engineering improvements or design modification, it may be necessary for the project to modify the safeguards design strategy to reduce or eliminate the risk.

By the end of conceptual design, the project also prepares a safeguards effectiveness report. This report documents the implementation of the safeguards design strategy and provides an evaluation of the safeguards effectiveness of the design. The report is structured so that portions of it evolve into the facility MC&A plan and the facility specific section of the Site Safeguards and Security Plan (SSSP). At the end of conceptual design, the customer reviews the safeguards effectiveness report and the other SBD reports and issues a Conceptual Safeguards Validation Report certifying that all the potential safeguards design issues have been identified, addressed, and resolved to a sufficient extent that the project can proceed to the next phase.

For facilities potentially subject to IAEA safeguards, the SBD process also mandates that the IAEA be notified of the intent to construct the facility as early as practicable in conceptual design. The SBD process also encourages collaboration with the IAEA regarding the information in the IAEA DIQ as early as practicable in the conceptual design. This will require an early decision from the IAEA whether the facility is to be placed under IAEA safeguards. For those facilities where the preferred design alternative is not selected until CD-1, this DIQ collaboration may need to be deferred until preliminary design. These issues are elaborated in Section 3.3 and Appendixes F and G.

3.2.3 Execution/Preliminary Design Phase (CD-1–CD-2)

During preliminary design, the various SBD reports (i.e., safeguards design strategy, vulnerability assessment, cyber security plan, MC&A process analysis, proliferation barrier analysis, safeguards effectiveness report, and safeguards risk and opportunity assessment) are updated to reflect the maturing design and any changes in DOE directives and policy (e.g., modification of the design basis threat). These

updated documents are produced by the end of preliminary design and are evaluated by the customer who documents this evaluation in Preliminary Safeguards Validation Report.

For facilities subject to IAEA safeguards, the SBD process includes development of the final DIQ and substantial negotiation of the Facility Attachment during this phase (see Section 3.3 and Appendixes F and G). This process is designed to permit the requirements for the SSC and design features needed to support the safeguards approach defined in the facility attachment to be incorporated during preliminary design. These requirements and their bases are documented in the update to the Safeguards Design Functions and Specifications for the facility.

3.2.4 Execution/Final Design Phase (CD-2–CD-3)

During final design, the various SBD reports (i.e., safeguards design strategy, vulnerability assessment, cybersecurity plan, MC&A process analysis, proliferation barrier analysis, safeguards effectiveness report, and safeguards risk and opportunity assessment) are updated to reflect the maturing design and any changes in DOE directives and policy (e.g., modification of the design basis threat). These updated documents are produced by the end of final design and are evaluated by the customer who documents this evaluation in Final Safeguards Design Validation Report.

For facilities subject to IAEA safeguards, the SBD process mandates negotiation of the final Facility Attachment during this phase. Changes to the requirements for supporting IAEA safeguards activities and their bases are documented in the update to the Safeguards Design Functions and Specifications for the facility (see Section 3.3 and Appendixes F and G).

3.2.5 Transition/Construction Phase (CD-3–CD-4)

During construction, the various SBD reports (i.e., safeguards design strategy, vulnerability assessment, cyber security plan, MC&A process analysis, proliferation barrier analysis, safeguards effectiveness report, and safeguards risk and opportunity assessment) are updated to reflect design changes, the increased understanding of facility operations, and any changes in DOE directives and policy (e.g., modification of the design basis threat). At this stage, the appropriate portions of the Safeguards Effectiveness Report are used to develop the facility MC&A Plan and the facility-specific revision to the SSSP. These updated documents are produced by the end of construction and are evaluated by the customer who documents this evaluation in the As-Built Safeguards Design Validation Report. With the transition to operations, the SBD process ends.

For facilities subject to IAEA safeguards, the SBD process mandates initiation of IAEA design information verification (DIV) activities and the delivery and installation of IAEA safeguards equipment during this phase. At the completion of construction, the SBD process anticipates that all equipment necessary for implementation of IAEA safeguards will have been installed (see Section 3.3 and Appendixes F and G). DIV will continue throughout the facility's operational lifetime.

3.2.6 Summary of SBD Steps for DOE Domestic Safeguards Environment

In summary, there are some 41 main steps making up the SBD process in support of DOE domestic requirements for facility design and construction. There are three iterations of the design phases (definition, preliminary, and final) and lastly facility construction, transition, startup, and closeout. The SBD process steps are listed in Table 3-1, as derived from Appendix E. These process steps for safeguards interact with DOE Program and Project Management and Project Engineering.

Table 3-1. Summary of main steps in the SBD process for DOE Domestic Environment. (The capital letters in brackets are used to identify process steps in the flowcharts, Figures E-1 to E-5, in Appendix E and have associated explanatory texts.)

Table 3-1. (continued).

Step No.	Main Steps - SBD Process
	Initiation Phase – Preconceptual Planning
1.	Appoint SBD Team Lead (A)
2.	Perform Preconceptual Safeguards Categorization (B)
3.	Document the SBD Tailoring Strategy (C)
4.	Seek DOE Expectations through their response to SBD Tailoring Strategy (D)
5.	Create SBD Team(s) (E)
CD-0	Approve Mission Need
6.	Generate and document Safeguards Design Strategy (SGDS) (F)
7.	SBD Team Input to Design Requirements (G)
8.	Participation in facility conceptual phase design studies (H)
9.	Perform SBD conceptual design activities within SBD Team (J)
10.	Participate in project, peer reviews of facility conceptual phase design (K)
11.	Perform a Safeguards Risk & Opportunities Assessment (L)
12.	Conduct Vulnerability Assessment(M)
13.	Document the Initial Cyber Security Plan (N)
14.	Develop Safeguards Design Functions & Specifications, inc. MC&A and Proliferation Barrier Analyses (P)
15.	Provide Safeguards Effectiveness Report (Q)
16.	Update Safeguards Design Strategy (R)
17.	Seek DOE to provide Conceptual Phase Safeguards Validation Report (S)
CD-1	DOE Design Process – First Critical Decision Point
18.	Perform SBD preliminary phase design activities within SBD Team (T)
19.	Participate facility preliminary phase design inc. detailed Safeguards Design Criteria (U)
20.	Participate in project, peer reviews of facility preliminary phase design (K)
21.	Update Safeguards Risk & Opportunities Assessment (L)
22.	Update Vulnerability Assessment and Cyber Security Plan (V, W)
23.	Update Safeguards Design Functions & Specifications, inc. MC&A and Proliferation Barrier Analyses (X)
24.	Update the Safeguards Effectiveness Report (Y)
25.	Update Safeguards Design Strategy (Z)
26.	Seek DOE to provide Preliminary Phase Safeguards Validation Report (AA)
CD-2	DOE Design Process – Second Critical Decision Point
27.	Perform SBD final phase design activities within SBD Team (BB)
28.	Participate facility final phase design including validation of design versus desired Functions & Requirements
29.	Participate in project, peer reviews of facility conceptual phase design (K)
30.	Update Safeguards Risk & Opportunities Assessment (L)
31.	Update Vulnerability Assessment and Cybersecurity Plan for final design (CC & DD)
32.	Update Safeguards Design Functions & Specifications, inc. MC&A and Proliferation

Table 3-1. (continued).

Step No.	Main Steps - SBD Process
	Barrier Analyses for final design (EE)
33.	Update the Safeguards Effectiveness Report for final design (FF)
34.	Update Safeguards Design Strategy for final design (GG)
35.	Seek DOE to provide Final Phase Safeguards Validation Report (HH)
CD-3	DOE Design Process – Third Critical Decision Point
36.	Safeguards activities (installation of equipment, verification of design implementation etc.) will be ongoing throughout construction (JJ)
37.	Independent evaluation of the readiness of completed facilities systems equipment procedures personnel and interfacing systems and organizations to begin operation (KK)
38.	Final update of Cybersecurity Plan (LL)
39.	As-Built Vulnerability Assessment Report (MM)
40.	Update to Final Safeguards Effectiveness Report (NN) and seek DOE acceptance of the final safeguards design (NN)
41.	Transition to Operations (PP)

3.3 Design and Construction Management with SBD Process for DOE Domestic Regulatory Environment and International Safeguards

As noted previously, the U.S. has voluntarily entered into obligations for IAEA safeguards requirements, so the effects of these must be incorporated into the SBD process for full compliance with DOE directives. Section 3.3 describes how IAEA requirements are used to perform the second stage of formulating the SBD process for domestic and international safeguards. Previously, Section 3.2 described how the DOE domestic prescriptive requirements together with the SBD team's performance safeguards requirements were used in an optioneering study to create the first stage of the SBD process.

3.3.1 Integration of Design and Construction Management with IAEA Safeguards Activities

The four principal activities for instituting IAEA safeguards—i.e., DIQ, facility attachment, safeguards approach, and DIV, see Section 2.4.2—can be integrated into the DOE acquisition system, as shown in Figure 3-2. The double-ended arrow shows that the DIQ is started as early as possible after CD-0. The remaining IAEA activities are generally associated with certain critical decision points within the DOE framework, but are also heavily dependent on the completion of previous IAEA activities. The dashed arrows in Figure 3-2 express the ongoing relationship between the IAEA and the owner/operator of the nuclear facility into the operation phase. Submission of the DIQ is the clear responsibility of the facility owner/operator gradating to the full responsibility of the IAEA for the facility attachment and DIV. However, all these require mutual cooperation in order to be effective.

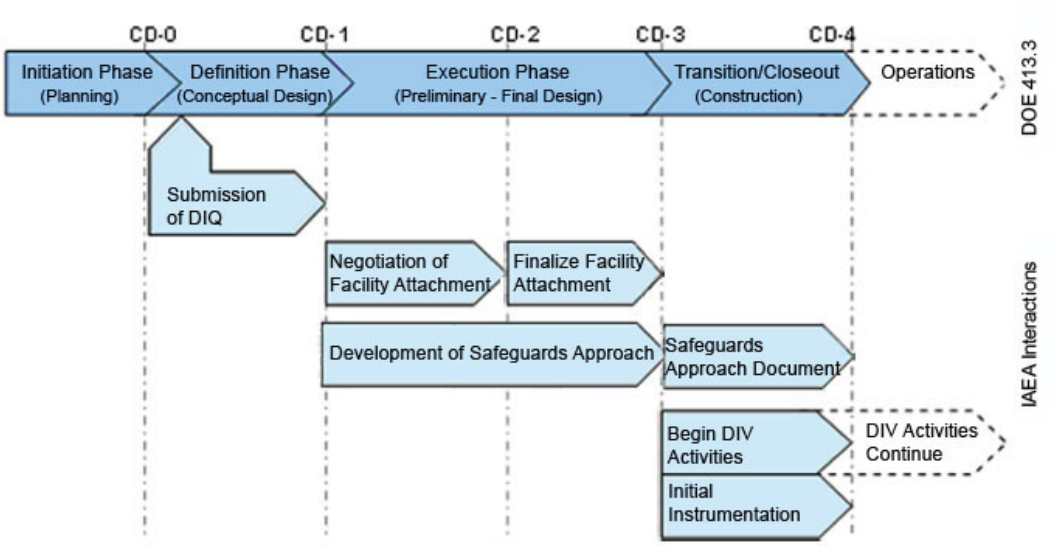


Figure 3-2. Integration of IAEA safeguards activities within the DOE acquisition system.

The IAEA safeguards points of interaction with DOE Program and Project Management, Project Engineering and Safeguards are shown in Appendix G, Figures G-1 through G-4. These provide detailed flowcharts, where for simplicity only three strata are shown on each figure for differing design stages. These flowcharts match up to the corresponding phased SBD process flowcharts given by Figures E-1 through E-5 in Appendix E. The two sets show all process steps for the SBD process with combined DOE domestic regulatory directives and international safeguards.

3.3.2 Definition/Conceptual Design Phase (CD-0–CD-1)

Following CD-0 approval, i.e., start of conceptual design, and for a nuclear weapons state, such as the U.S., there is an early determination of whether to place the planned facility on the EFL. If so, the IAEA is notified of the Intent for Facility. The process by which DOE makes additions and deletions to the list of DOE facilities eligible for IAEA inspection under the VOA is shown schematically in DOE M 142.2-1, 9-4-08 (page III-2, Figure III-1). Duties are placed on various DOE administrators and officers including that participation with the Office of International Regimes and Agreements "will take account of, from inception, IAEA Safeguards requirements and whether the facility would be placed on the eligible list." DOE M 142.2-1, 9-4-08 (page III-3). The list shows nuclear facilities agreed to be open to IAEA safeguards activities including inspections on all source or special fissionable material. The eligible facilities are not associated with activities with direct national security significance to the United States. From this list, the IAEA may choose to inspect a facility based on a need to verify information provided by the licensee.

In the DOE context, the U.S. requirement for submission of the DIQ is specified in DOE O 142.2A (especially Attachment 2) and DOE M 142.2-1 (Approved 9-4-2008). In the commercial arena, the appropriate regulation is provided by 10 CFR 75. The DIQ form is designated as Form N-91 (IAEA Form N-91, 6-2005). This form is required as soon as the decision is made to build the facility corresponding to CD-0. Models and examples of completed DIQs are given (SAC 1979).

The DOE acquisition process integrated with the SBD process identifies intrinsic features that are necessary to allow proper IAEA verification and are included, as necessary, early in the design process to minimize any later costly redesign and retrofit efforts. Early notification to the IAEA to allow the international processes to begin is important. The project management process, DOE M 413.3-1, establishes the preferred design alternative for the facility by the time of CD-1 approval. DOE

Standard 1189-2008 emphasizes the importance of establishing the facility arrangement by no later than CD-1. This means there is considerable urgency for the IAEA interaction to support this schedule without fail, particularly insofar as major facility alternatives and infrastructure needs are concerned. If this is not possible, then transmission of the DIQ may move into the CD-1 phase.

3.3.3 Execution/Preliminary Design Phase (CD-1–CD-2)

The DIQ is completed based on conceptual design work, including safeguards SSC, as prepared for CD-1. The IAEA involvement begins in earnest with the transmission of the DIQ. Transmittal of the DIQ to the IAEA requires coordination between the design team, national regulatory agencies (e.g., DOE), and state-level organizations (e.g., U.S. State Department).

Either starting in conceptual or preliminary design, the IAEA commences review of the DIQ and other relevant design information at IAEA Headquarters in Vienna. It then transmits a list of questions regarding any apparent inconsistencies or about safeguards relevant features and may repeat DIE activities at the designer's office or at the facility site during the early stages of site clearing, as required. IAEA schedules DIE activities at the facility with the national regulatory authorities.

After submitting the initial DIQ, the national authorities and field element (DOE-regulated) or facility operator (NRC-regulated in U.S.) begin discussing and negotiating the Subsidiary Arrangements relevant to the facility being constructed. The Subsidiary Arrangements consist of a General Part, applicable to all common nuclear activities of the country, and a Facility Attachment, prepared for each facility in the country and describing arrangements specific for that facility (IAEA Safeguards Glossary – 2001 Edition, "Subsidiary Arrangements," Paragraph 1.26).

The facility attachment is a negotiated document between the IAEA and the State regarding the design features (intrinsic and extrinsic) that will be incorporated into the particular nuclear facility to accommodate the IAEA verification activities during construction and operation. Not addressing these issues satisfactorily at an early enough stage in the process may result in the construction of a facility in which international (IAEA) safeguards are not practicable to operate, which could have serious ramifications for a country that is a declared party to the NPT. The designer commences preparation of the facility attachment during preliminary design. The facility attachment and the plant design should be aligned, cover aspects such as laboratory space, conduits, footprint of hot cells, IAEA instrument space, Inspector office, and be available in a timely fashion to allow the detailed design efforts to proceed. The facility attachment to physical plant is jointly completed for the preliminary design phase.

3.3.4 Execution/Final Design Phase (CD-2 – CD-3)

As the design effort progresses to finer detail, so does the IAEA facility attachment input. As the facility design is optimized and reviewed for final approval, the IAEA input is finalized and incorporated into the overall design. The negotiation of the facility attachment spans the duration of design, construction, and commissioning of the facility and represents the greatest challenge to SBD to coordinate with the facility activities. For application of IAEA safeguards to a DOE facility, NNSA and other DOE officials become part of the process, as spelled out in the VOA.

3.3.5 Transition – Closeout/Construction Phase (CD-3 – CD-4)

As construction begins, DIE and DIV activities will be performed by the IAEA through all stages of construction and will continue as needed during operation. As the facility is built and prepared for operation, the IAEA equipment needs to be delivered and installed (including testing, tamper-proofing, initial calibrations). No steps are shown here relating to the safeguards approach as this is an IAEA responsibility.

3.3.6 Summarizing International Safeguards Steps in SBD Process

In conclusion, some 14 additional, main steps are incorporated into the SBD process to account for the IAEA safeguards requirements in support of DOE facility acquisition. Again, there are three iterations of the design phases (definition, preliminary, and final) and lastly facility construction, transition, startup, and closeout. The SBD process steps responding to international requirements are listed in Table 3-2, as derived from Appendix G. These process steps complete the SBD process for integration with DOE Program and Project Management and Project Engineering.

Table 3-2. Summary of additional main steps in SBD process for domestic and international requirements. (The capital letters in brackets are used to identify process steps in the flowcharts, Figures G-1 to G-4, in Appendix G and have associated explanatory texts.)

Step No.	Main Steps – SBD Process
CD-0	Approve Mission Need
1.	Determination of whether to place the planned facility on Eligible (nuclear) Facility List
2.	Notify IAEA of Intent for Facility (QQ)
3.	Potential early start to preparation of Design Information Questionnaire (RR´)
4.	Potential early transmission of Design Information Questionnaire to IAEA (RR´)
CD-1	DOE Design Process – First Critical Decision Point
5.	Prepare Design Information Questionnaire (RR)
6.	Transmit Design Information Questionnaire to IAEA (RR)
7.	Develop Facility Attachment (SS)
8.	Negotiate Facility Attachment information with IAEA (SS)
9.	Finalize IAEA Facility Attachment Input to physical plant (TT)
CD-2	DOE Design Process – Second Critical Decision Point
10.	Final Facility Attachment input to IAEA (UU)
11.	Submission of Program Requirements Document for construction/projects being executed by NNSA (PRD)
CD-3	DOE Design Process – Third Critical Decision Point
12.	IAEA undertakes Design Information Verification activities (VV)
13.	Delivery of IAEA safeguards equipment to facility (WW)
14.	Installation of IAEA safeguards equipment in facility (WW)

The mechanism and extent for IAEA participation in a SBD process for DOE design and construction, for example, does depend on effective arrangements to deal with intellectual property restrictions, commercial matters, and development of unclassified facility design, including safeguards and documents. On adoption of a global standard for SBD, the same issues will arise but probably from a differing perspective.

3.4 Complete SBD Process for DOE Environment

The study generated an integrated SBD process covering DOE domestic regulatory directives and international (IAEA) safeguards for a DOE design and construction management environment. It comprises 55 process steps, which are shown in two series of flowcharts (see Appendixes E and G). This approach tested the adaptability and assessed effectiveness of the SBD process in an appropriate environment, i.e., the DOE system for acquisition of capital assets. Although directives have not been

drafted for use of SBD within the DOE acquisition system, the SBD process is considered to be sufficiently developed to be tested on a pilot scale within an actual DOE project. This would check and improve process viability and help determine the best way to effect institutionalization within the DOE environment. The methodology used is recommended for the shaping of the SBD process to other design and construction environments in the U.S. such as that for commercial facilities regulated by the NRC.

The two-stage approach also suits institutionalization that addresses specifically the integration with international safeguards, because from the IAEA's perspective, the DOE regulatory system is an example of what the IAEA calls the SSAC of nuclear material. The agency responsible for the SSAC is usually the IAEA's principal interface for international safeguards. The methodology used to form the overall SBD process for the DOE environment may be used to combine a given state's regulatory requirements with the IAEA requirements to form an SBD process adapted to a State and its SSAC.

The above SBD process developed within the DOE environment for domestic directives and international safeguards is a simple, concise, formalized, and integrated approach. Discussion with stakeholders will help validate the proposed approach. Further work will formalize lower-level requirements. Pilot testing is recommended to confirm performance within actual projects as well as to seek improvements.

4. TECHNOLOGY AND METHODOLOGY SUPPORTING SAFEGUARDS-BY-DESIGN

Several high-level potential prescriptive requirements for proliferation resistance or safeguardability were identified in Section 2.2. Methodologies for assessing measures for application to facility designs are under development and not yet well accepted by regulators and industry. The SBD process is shown to have flexibility to enable parallel testing and methodology development. Section 4 describes links to the Next Generation Safeguards Initiative (NGSI), related work at the IAEA, needs for and progress with technical solutions, guiding principles, and a summary of best practices and lessons learned relevant to SBD.

4.1 Proliferation Resistance and Safeguardability

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" (IAEA 2002). No nuclear energy system can be proliferation proof, but different systems can present varying degrees of proliferation risk because of the combined actions of the proliferation barriers acting in that system. Institutions and states can erect and maintain institutional barriers to proliferation—examples of such extrinsic measures include treaties, commercial and legal arrangements, export controls, actions to support United Nations Resolution 1540, and notably also the application of international safeguards by the IAEA.

Designers can contribute to proliferation risk reduction through the selection of processes and incorporation of facility design characteristics, i.e. intrinsic features, that either directly impede proliferation pathways or facilitate the application of other extrinsic measures, like international safeguards. Intrinsic features include inherent physical properties of the system and are in general very robust and desirable because they are very difficult to modify or overcome. (Generation IV International Forum/PRPP Expert Group 2006)

A nuclear energy system's proliferation resistance may vary according to the specific threat and results from the combined effect of all its different barriers. For present purposes, it is convenient to discuss proliferation resistance as resulting from the application of international safeguards plus other proliferation barriers. The incorporation of these other proliferation barriers in facility and process design can be readily dealt with in the proposed SBD process so long as relevant requirements are articulated, formalized, and included in the design process. That is not presently the case. however, future efforts must be directed at defining sensible requirements and establishing the methods by which system performance against these requirements can be assessed.

4.1.1 Measures by Which to Gauge Proliferation Resistance

Particularly important and useful products of the methodology developed by the PR&PP expert group of the Generation IV International Forum are the creation of a vocabulary for the discussion of proliferation resistance and the development of proposed high-level measures of proliferation resistance. This group proposed six such measures.

Two measures relate specifically to the application of international safeguards to the nuclear energy system:

1. Detection Probability. The cumulative probability of detecting a proliferation segment or pathway.
2. Detection Resource Efficiency. The efficiency in the use of staffing, equipment, and funding to apply international safeguards to the nuclear energy system.

The PR&PP group further suggests using the measure of safeguardability to replace these two measures for the case of future nuclear energy systems. Safeguardability is "the ease with which the system can be effectively and efficiently placed under international safeguards." (Gen IV, PRPPWG/2006/005 Rev. 5) All these safeguards-related measures suggest the design importance of designing facilities to make it easier to apply safeguards that are efficient and effective.

Three of the proposed measures describe other barriers presented by the system to the proliferator:

1. 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.
2. Proliferation Cost. The economic and staffing investment required to overcome the multiple technical barriers to proliferation including the use of existing or new facilities.
3. 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).

These measures suggest the design objective of making it technically difficult, time consuming, and costly for the potential proliferator to exploit the nuclear energy system.

The final measure is Fissile Material Type, defined as "a categorization of material based on the degree to which its characteristics affect its utility for use in nuclear explosives." (Gen IV, PRPPWG/2006/005 Rev. 5) This measure is essentially established by the fuel cycle properties.

This particular set of measures for proliferation resistance are useful today, but for the reasons described in Section 4.1.3, it is likely they will further evolve and mature with testing and use.

Commonalities between Safety Analysis and Proliferation Resistance & Physical Protection (Gen IV, IF/PRPPWG/2006/005, 2006)

The Generation IV program established four primary goals for Sustainability, Economics, Safety and Reliability, and Proliferation Resistance and Physical Protection. This PR&PP Methodology Report describes the process used to establish the approach to evaluate PR&PP. Similar processes are used to evaluate and compare safety and reliability; it is recommended that the analyses be done in parallel. The following familiar graphic defines the PR/PP methodological approach:

THREATS → SYSTEM RESPONSE → OUTCOMES

The accident analysis process can be defined in a similar way:

ACCIDENT INITIATORS → SYSTEM RESPONSE → CONSEQUENCES

As these paradigms illustrate, each of the two types of assessments requires similar system information to be collected and analyzed at various stages of facility design, development, and construction. Parallel evaluations in these areas complement each other, and the results of these studies and their implementation interrelate and affect each other. For a PR&PP evaluation, the appropriate time for early system element and target identification is at the time the facility hazard evaluation (safety assessment) is done as a part of the accident analysis process. The hazard evaluation

- Establishes the maximum quantity of material involved, including its form and possible locations
- Identifies potential initiating events that could affect the hazardous material and lead to a release
- Describes structures, systems, or components that serve to prevent the release of hazardous material in an accident scenario
- Identifies structures, systems, or components that serve to mitigate the consequences of a release of hazardous materials in an accident scenario.

There are obvious parallels in this process to identifying and categorizing targets for both the PP and the PR assessment processes.

4.1.2 Safeguardability as a Design Goal

The incorporation of design and process features that makes it easier and less expensive to apply safeguards that are effective and efficient is a foundational objective of the SBD process. Broad application of a mature SBD process, therefore, will directly support key objectives of the NGSI and the IAEA.

4.1.3 Approaches for Evaluating Proliferation Resistance

The attendees of the Como II conference held in 2002 in Como, Italy, foresaw that a mix of methodological approaches should be developed and used to define and assess the performance of nuclear energy systems of the future. (IAEA 2002) They suggested a three-pronged approach to assessment methodology for proliferation resistance and physical protection—a checklist approach, a qualitative approach, and a quantitative assessment approach. In the ensuing years substantial progress has been made toward developing methodologies for all three of these approaches. The IAEA-led INPRO program has developed the checklist approach, while the PR&PP group has pursued development of a risk-informed methodology for both the qualitative and quantitative assessment approaches. (Generation IV International Forum/PRPP Expert Group, 2006)

The checklist approach considers specific system design characteristics or properties, one at a time. The PR&PP methodology on the other hand calls for a holistic, risk-informed analysis that examines the relative performance of whole nuclear energy systems. Both methodologies are useful today, are proving to be complementary in their use, and both continue to evolve. (Pomeroy et al. 2008) However, 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. For this reason, a risk-informed, holistic analysis approach—like that advocated by the PR&PP methodology—is particularly well suited for application in the SBD process.

Safeguardability

(Gen IV, GIF/PRPPWG/2006/005, 2006)

Three Categories for Safeguards Implementation:

1. Attributes for potential ease of performing Design Information Verification;
2. Attributes for potential ease of performing Nuclear Material Accounting;
3. Attributes for potential ease of implementing Containment & Surveillance Measures.

System Attributes enhancing Safeguardability

Facilitate DIV - Transparency of layout, Use of 3d scenario reconstruction models, Visual access to facility equipment while operational and Comprehensiveness of facility documentation and data

Facilitate Nuclear Material Accounting – Uniqueness/hardness of material signature, Feasibility of passive measurement methods, Item/bulk, Uncertainties of detection equipment, Annual Throughput, Batch or continuous process, Material heat generation rate,, Radiation field, Amount of hidden inventory and possibility NRTA implementation.

Facilitate Containment & Surveillance (C/S) Measures – Operational practice, Extent of Automation, Standardization of Items in transit, Possibility to apply remote monitoring.

It is customary in risk-informed approaches for design and assessment to begin by constructing event trees to describe the possible strategies (pathways) that an adversary might exploit in order to achieve the desired objectives. In cases where design details are scarce, where project resources are limited, or where the formal performance requirements and assessment methodology may not yet be fully mature, the process of constructing and inspecting the event trees in a disciplined fashion—combined with expert judgment—is a reasonable approach to identifying and estimating vulnerabilities and then allocating resources to mitigate them. This type of analysis should not await development of detailed designs. Rather as the level of design detail increases the definitions of the events considered also change to keep pace with the current level of detail. As the design progresses and more design details become available, that information can be used in more rigorous, quantitative analysis of performance of the system as a whole, and should include consideration of uncertainties. This graded, iterative approach to SBD as proposed here is illustrated in Figure 3-1.

4.2 Lessons Learned from the Evolution of Risk-Informed Nuclear Safety Regulation

Appendix C, "Evolving Approach to Nuclear Safety," summarizes the evolution of the risk-informed approach to safety over recent decades. This evolution, and its foundation upon probabilistic risk assessment, has lessons relevant and useful for managing the maturation of the SBD process. In planning this process, each factor listed below should be recognized and accommodated. Among the most important lessons are the following:

The acceptance of use of probabilistic risk assessment in various industries and settings has been a slow process, impeded by the unfamiliarity and complexity of the method, and sometimes by its role as bearer of unwelcomed news.

The great value of probabilistic risk assessment is in its ability to provide an integrated assessment of a system's performance, taking into account all factors that an analyst may consider to be important. This assessment can include the effects of uncertainties, sensitivities, and the importance of the various factors affecting the results provided. It provides a systematic approach for identifying vulnerabilities and for guiding resources to mitigate them.

When used in an undisciplined fashion any modeling treatment can yield unreliable results (as with use of rosy inputs and assumptions). Only after performance of many similar analyses and comparison of their results and sensitivities has it been feasible for consensus to emerge concerning safety analyses. This experience has permitted creation of understanding of essential elements and treatments that should be expected in a high quality analysis and has retarded use of probabilistic risk assessment in generating falsely optimistic results. Short cuts to reaching such a stage of understanding do not exist, either in safety or nonproliferation applications.

Considerable investments are required for creation of the needed body of data, library of models and analytical tools, and the cadre of seasoned analysts in order to support performance and cross examination of many analyses. Also, once created, these analytical assets must be sustained through consistent use, or they will atrophy.

The implications of these lessons for SBD are reasonably obvious, as its further development appears likely to parallel that of the treatment of safety. Doubts that this maturation into a valuable treatment of proliferation problems is feasible are as unfounded as the belief that it can occur easily.

4.3 SBD and the NNSA Next Generation Safeguards Roadmap

4.3.1 Support to NGSI

The demonstration and institutionalizing of the SBD process is a fundamental element of the Next Generation ("NextGen") Safeguards Roadmap prepared by the U.S. DOE National Nuclear Security Administration Office of NA-24. The strength of this connection is clearly shown in the excerpt from the "Safeguards Concepts and Approaches" section of the Safeguards Roadmap, as quoted below:

> The development of advanced safeguards approaches and concepts will support the Next Generation Safeguards Initiative (NGSI) by paving the way for, and promoting, the use of advanced safeguards methods, innovations and technology. This is made more urgent in an era of expanding nuclear infrastructure and spread of sensitive nuclear technology. Such approaches would meet and support international safeguards requirements and be consistent with established best practices for verifying and monitoring nuclear material and facilities. New approaches and concepts will be consistent with the IAEA focus on state-level and integrated safeguards. The role of multi-lateral and regional safeguards partnerships, as a complement to the IAEA international safeguards regime, will also be considered.
>
> **Objective 1: Demonstrate and Institutionalize Safeguards-by-Design**
>
> The SBD approach requires the identification and integration of safeguards requirements (in addition to security, physical protection, and safety requirements) into the design of a nuclear facility at the earliest stages of conceptual design. Effective implementation of SBD would avoid expensive and time-consuming retrofitting of a facility during and after startup and operation. DOE will promote SBD as an international norm and standardized process to ensure the timely, efficient, and cost-effective implementation of safeguards,

safety, and physical protection features. The concept of SBD should also focus on the idea that efficient design for safeguards will make it easier for an operator and state to perform satisfactory nuclear MC&A, which can reap economical advantages for the facility operator. Hence, good safeguards design can mean good business practice.

Guidelines, Requirements, and Best Practices. The 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 (e.g., standardized surveillance systems for spent fuel ponds). Definitive domestic and international safeguards requirements would also address regulatory gaps (e.g., NRC regulations for commercial fuel reprocessing and mixed oxide fuel fabrication in the United States).

Best practices should catalog to the extent possible facility design features necessary to implement effective safeguards. Examples of relevant design issues include designing ventilation ductwork, filtration systems, and process piping to minimize fissile material, e.g. plutonium, holdup. It is envisioned that the catalog of best practices would start at a general design level and become more elaborate and detailed, based on the input from international working groups addressing this subject.

Demonstrate Safeguards-by-Design at a New Nuclear Facility in the United States or in a Foreign Country. Demonstration of SBD on a pilot scale could help promote broader acceptance of the overall approach, both in the United States and internationally. Opportunities for demonstrating SBD include facilities under consideration as part of programs to promote nuclear energy expansion, such as the proposed AFCF or Consolidated Fuel Treatment Center.

So, the demonstration and institutionalizing of SBD is a major new safeguards concept and approach supported by U.S. DOE/NNSA, as articulated in their Next Generation Safeguards Roadmap.

4.4 SBD and Related Work at the IAEA

Work is also being conducted at the IAEA pursuing an SBD methodology and process. In October of 2008, an international "Workshop on Facility Design and Plant Operation Features that Facilitate the Implementation of IAEA Safeguards" was held where SBD was a major topic. International safeguards experts from the IAEA and from around the world gathered at this workshop with the goal of defining common objectives and a vision for mapping a prospective strategy for implementation. An IAEA symposium was held in Vienna, Austria, which also featured SBD. The strength of the connection between "Safeguards-by-Design," as articulated by NNSA, the ISBD Team, and the International Workshop Team, is shown in the excerpt of the draft report from the workshop, as quoted below:

> Overview of the Safeguards-by-Design Process
>
> Safeguards-by-design is defined by the IAEA as an approach whereby international safeguards is fully integrated into the overall design process of a nuclear facility, from initial planning, through design, construction, and operation.
>
> Examination of the processes for design and construction, and for the development and application of the Safeguards Approach for a given facility,

illustrate the importance of integrating safeguards considerations into the project structure for the design and construction of the facility from the very inception. In so doing, the disciplined application of proven project management and systems engineering principles will be very important.

There are three different categories of nuclear facilities according to their developmental status: Existing, Evolutionary and Developmental. Existing facilities are built and operating, with operational safeguards, and the only realistic prospect for change is in the optimization of operations and extrinsic measures for safeguards. However, existing facilities are extremely important to a safeguards-by-design program, because they provide the experience base ('prior art' and 'best practice') that can be researched to provide information, documents, and requirements of vital importance to the application of the safeguards-by-design process in future facilities, i.e., knowledge management. This information includes best practices (for both safeguards and facility design), design guidelines (collection of design principles that will be useful to the safeguards and designer community), and safeguards related design requirements and the associated acceptance criteria.

New, evolutionary facilities by definition, involve only modest revisions from existing, operating facilities for which Safeguards Approaches already exist. Changes to both the facility design and Safeguards Approach are possible, in principle, although as a practical matter many such projects might only permit minor design changes. For these projects, it is expected to be highly beneficial to include safeguards requirements, activities, and interactions in the formal project planning and execution, thereby reducing risks to project performance measured in cost, schedule and by the safeguards systems' effectiveness.

New developmental facilities involve substantially new design features and technologies, which will require new safeguards approaches. They offer the greatest potential for early and beneficial application of safeguards by design. The IAEA should provide high-level performance oriented requirements for safeguards that are written in a form that will be useful to designers during the development process. Analysis of systems and safeguards performance (e.g., safeguards efficiency and effectiveness) can be gainfully applied to inform the selection of design features and safeguards approaches that minimize life cycle costs. Likewise, as R&D is demonstrated in practice and technology is employed in a new facility project, enhanced interaction between designers and the IAEA is foreseen to be both possible and beneficial. As above, safeguards requirements, activities and interactions should be included in the formal project planning and execution, thereby reducing the risks to project performance.

As can be seen in this discussion of the Safeguards-by-Design process and framework, the overall vision and purpose of the process as seen by NNSA, the DOE National Laboratory ISBD Team, the IAEA and international community is comparable. Broad recognition of specific safeguards requirements, especially for international safeguards, need to be better articulated and understood by the designers of nuclear facilities. This becomes more important as facilities become more complex requiring that safeguards measures be in place and installed while the facility is under construction. The International Workshop team discussed how this will depend on the maturity of the facility design, i.e., whether the facility is existing, evolutionary, or developmental. This appears broadly applicable, although the ISBD Team envisions that even facilities of a proven design may need the latest safeguards features and equipment incorporated into the facility design. By example, even though new gas centrifuge enrichment plants and mixed oxide fuel fabrication plants of a proven process design are being constructed in the

world today, the ISBD Team envisions that these facilities would still benefit from the SBD process and methodology. The SBD process should not be seen as something solely relevant to new developmental nuclear facilities only on the drawing board.

In summary, the NNSA Next Generation Roadmap and the current work at the IAEA underscore the need and value of an SBD process—for ensuring that the design and construction of new nuclear facilities is efficient and that these designs incorporate the necessary features for the effective application of nuclear safeguards throughout the world.

4.5 Needs for Development of Technical Solutions

Supporting methodology development is required because no methods are formally accepted, domestically or internationally, for assessment of proliferation barriers and safeguardability of nuclear facilities as needed for application of the SBD process. Without accepted methodologies, safeguards requirements cannot be quantitatively evaluated and no strong case can be made for safeguards-driven selection of fundamental facility design options such as fuel cycle, process, flowsheet, and remote maintenance philosophy. Without accepted proliferation resistance requirements and accepted assessment methodology, SBD has little influence on the selection of facility alternatives unless they are cost neutral. Essentially, SBD is already feasible under the domestic physical protection area. Some parties perceive it to be so under the international safeguards area once the facility layout, process, and major equipment have been adopted, e.g., recent reprocessing facilities. The latter, of course, removes the full potential benefit of SBD. For gas centrifuge enrichment plants with strong commercial confidentiality concerns, early conceptual design for online safeguards instrumentation and other Material Balance Areas monitoring in halls is particularly difficult to establish without well-justified proliferation barrier requirements. Methodologies under development worldwide include the PR-PP Methodology of the Generation IV Industrial Forum and the INPRO approach developed by an IAEA-led team. The two are currently undergoing joint review and coordination. However, based on the earlier formalization and culture shift for safety-in-design, full regulatory and industrial acceptance of SBD may take the best part of a decade and respond to the needs-driven pilot testing of the SBD process. Pure replication of the safety-in-design approach for SBD is not expected to be possible due to widely differing performance and prescriptive requirements and psychology, human performance, and limitations in fault tree treatment for risk assessment.

The current SBD approach is expected to accommodate most new proliferation resistance requirements and evaluation methodologies. High-level performance requirements for the SBD process were identified but found to be mainly qualitative in nature, which contrasts with lower-level prescriptive requirements, e.g., DOE physical protection directives. More detailed and semiquantitative requirements are likely to be needed to enable SBD process optimization.

Several concepts for the tailoring of the SBD generic process to the U.S. commercial arena under NRC regulation have been explored. In principle, the SBD process is flexible enough to meet this situation, see Appendix K. However, tailoring of the SBD process to the NRC regulatory pattern has not yet been performed and may raise issues generically. In this sense, it may be valuable to approach the goal of a new global SBD standard within the baseline safeguards performance requirements of physical protection, MC& A, and the International Safeguards requirements of DOE, NRC, IAEA, together with other major and developing nuclear countries, e.g., Canada, China, France, Japan, Russian Federation, South Korea, and the United Kingdom.

4.6 Safeguards-by-Design Guiding Principles

To apply the SBD process to a particular nuclear facility design, experience with project management, systems engineering, and safeguards leads to a preliminary set of guidelines or principles.

These guiding principles apply to all nuclear facility design efforts and serve to enhance the consistency with which SBD provides benefit to any given project. A similar set of guiding principles for applying the Safety-in-Design standard is shown in Appendix I for comparison. The proposed preliminary SBD guiding principles are:

1. Establishment of the safeguards design team with proper expertise and at the earliest phases of the project.
2. Early and complete incorporation of the relevant safeguards regulations and requirements into the overall project requirements.
3. All stakeholders are included and agree on timetables, deadlines, and hold points for resolution of safeguards issues.
4. The key stakeholder provides documented validation of the safeguards deliverables at each hold--point.
5. The safeguards team is integrated with the other project teams to enhance design effectiveness and improve cost and schedule estimates
6. Selection and optimization between various safeguards design principles and corresponding options is performed using life-cycle cost analysis, some examples of principles and options are given below:
    a. Recognize that intrinsic features are generally preferred over extrinsic systems.
    b. Multiple barriers providing defense-in-depth are normally preferred.
    c. Prevention of loss or theft is preferable to mitigation.
    d. Design for minimum capability throughout facility consistent with requirements.
    e. Nuclear materials inventories should be minimized consistent with facility objectives.
    f. Recognize that underground location of facilities or their key parts and layouts with materials in interior locations may be superior.
    g. Documented best practices are referenced to compare alternatives.
    h. Flexibility in design.
    i. Design to address future upgrades, and regulatory and production changes.
    j. Provide high speed data transmission and plug'n'play capabilities.
    k. Provide a high reliability uninterruptible power supply.
7. Important safeguards features or functions are identified during earliest design phases.
8. The safeguards team and design teams provide sufficient detail to enable major cost drivers, risks, and opportunities of the alternatives to be addressed. Not all details will be available in the early stages. Additional detail and documentation must be included as it emerges.
9. Recognized and approved codes, standards, and analyses are to be used.
10. The bases for alternatives selection, including how each choice improves the safeguards for the facility are to be documented within the project records.

4.7 Summary of Best Practices and Lesson Learned

A "best practice" is a process, practice, or system identified in an organization that performs exceptionally well and is widely recognized as improving the performance and efficiency of organizations in specific areas. A "lesson learned" documents the experience gained from working with or solving real-world problems, for example during a project, and is typically negative with respect to identifying process, practice, or systems to use in specific situations.

Six major projects were examined to mine information of relevance to the ISBD Team. The principal conclusions from these examples of best practice (first five) and lessons learned (last one) are as follows:

Rokkashomura Reprocessing Plant (RRP)—The IAEA safeguards system for RRP represents a world best practice as developed from long plant experience, several international development reviews, and an earlier major pilot reprocessing facility in Japan. The RRP was developed from La Hague reprocessing plants that were designed and developed, including safeguards aspects, over several generations of facilities in an evolutionary environment spanning about five decades. SBD as defined by an early safeguards design effort in parallel with process, equipment, and facility design, may have less beneficial impact where overall design is largely unchanged from one facility to the next, although regulatory differences usually exist between different countries. IAEA safeguards at RRP are deemed to be effective, but possibly not as cost effective as would have been the case where safeguards were fully integrated into design from the preconceptual planning stage. Even with extended IAEA consultation with Japanese Nuclear Fuel Limited (JNFL), design and implementation of the software integration for the data collection and evaluation systems was started late in the process.

Mixed Oxide Fuel Fabrication Facility (MFFF)—The evolutionary design and operational background of French technology contributing to the MFFF at Savannah River reduced the benefit of SBD involvement where, excepting different U.S. regulatory requirements, significant replication occurred from one plant to another. While safeguards designs for the French facilities were probably more evolutionary than SBD process oriented, design integration and SBD took some part in MFFF design because of knowledge learned during the design of MELOX (mélange oxide) facilities. SBD has the potential to provide the greatest benefit where a developmental approach is being used for facility design.

Next Generation Facilities—SBD has the potential to give greatest benefit where facility design is being conducted using a "clean-sheet" approach and design options selection (e.g., flowsheet, equipment selection, and layout) is less constrained by existing practice. Next generation plants are also more likely to be given more radical or "step-change" design requirements supported by directed research and development calling for innovative concepts, i.e., developmental nuclear facilities. This best practice is derived from several sources including Section 5.2, Related Work at IAEA, and the RRP and Savannah River MFFF best practices given in this subsection.

Development of Unclassified (UCNI) Design Requirements for Safeguards—A recent best practice from a DOE facility project concerns design practice in the preliminary phase. The vulnerability assessment is classified, which compartmentalizes information since designers are not security cleared. It also inhibits use of systems engineering tools due to the need for operation on classified computer systems. As the solution, an unclassified (UCNI) design requirements document has been developed from the vulnerability assessment, which is similar to a part of the preliminary documented safety analysis/documented safety analysis. Designers are better able to understand the safeguards requirements, without full knowledge of their bases, and identify areas where it appears that the safeguards requirements are driving the design in a non-optimal direction. Designers ensure that all requirements are captured in the initial design rather than being "patched in" later through the comment process. This also enables vulnerability assessment -derived requirements to be used in systems engineering and requirements management tools. This is a simple, but powerful, development in the standard DOE approach with the potential to significantly enhance SBD and with wider application, e.g., proliferation barrier analysis.

Safeguards Integration—Historically, it has been common to divide safeguards activities into two broad categories: security (physical protection) and MC&A, which have been regulated or licensed as separate entities by DOE and NRC, respectively. These two categories cover many detailed topics. Recently, these two categories have been extended somewhat by definition as physical protection

robustness and proliferation resistance. The former relates to threats from subnationals, and the latter relates to threats from owner nation-states. The focus of integration of safeguards changes with time depending on contemporary challenges and a wide range of approaches have been proposed over the past several decades. Safeguards and security comprise or are affected by so many inter-related aspects or parts that integration to a single entity may be difficult and priorities and best-fit must govern. As an example, success in integration of data needs has been successful to the point of being considered routine while other proposals, such as integrating physical protection with material transfer, are not used.

Sellafield Thermal Oxide Reprocessing Plant—The prolonged highly radioactive liquor leakage into the feed clarification process cell, which was found in April 2005 at the THORP commercial oxide fuel reprocessing plant in the United Kingdom, showed weaknesses in the design process, facility design, plant monitoring and operation, operational and management cultures, safeguards modeling, and safety culture (HSE, 2007). Approximately 83 m^3 (109 yd^3) of dissolver product liquor, containing approximately 22 tons of spent nuclear fuel (including approximately 160 kg [Pu])), leaked onto the floor of the cell. The leak began prior to August 28, 2004, and remained undiscovered until April 20, 2005. The leak came from a pipe, which had completely severed just above where it entered one of the two head end accountancy tanks. The most likely cause was fatigue failure from the swinging/swaying motion of the suspended tank, which occurred during agitation of the tank contents as part of normal operation. While SBD is a valuable integrating technique (and might possibly have helped avoid the initiating failure), this lesson learned demonstrates the importance of wider integration across the whole facility life cycle including design (part of which is RAMI [reliability, availability, maintainability, and inspectability] assessment), commissioning, operations, and safeguards activities (especially MC&A and modeling).

Greater detail on these cases is given in Appendix H. Several text boxes interspersed in the report provide additional best practices, etc.

5. INSTITUTIONALIZING SAFEGUARDS-BY-DESIGN

5.1 Progress in FY 2008

Section 1 listed the ISBD FY-08 project work plan scope items. This section describes progress and shows how the scope items of the ISBD FY 2008 project work plan are tracked. Table 5-1 links the seven scope items, A–G, of the ISBD FY 2008 project work plan to particular sections of the report and the four categories of work under the ISBD framework: institutionalization, requirements definition, design processes, and technology and methodology. Institutionalization is the enabling foundation for the other three technical categories, see Figure 1-2. In Section 5.2, the focus is placed on institutionalization and future options. Section 7 selects the recommended path forward.

Being research and development, the ISBD FY-08 project extended the seven scope items, A–G, in two areas where it was found effective to do so to prepare the way for promising avenues in FY-09. These two additional areas are shown as H and I in Table 5-1. The NNSA sponsor favors application of SDB to commercial practice in the U.S., especially because a significant number of fuel cycle facility projects are in various stages of planning, design and construction (see Appendix K). The preparation of a generic SBD process was an innovation of the SBD team that was stimulated by the studies for DOE design and construction management with SBD process and the need to apply SBD to a variety of domestic and foreign state regulatory environments (see Section 6).

Table 5-1. Tracking ISBD FY 2008 work scope items.

Scope Items for FY 2008 ISBD	**Scope Met in Report #**	**ISBD Framework Categories**
A. High-level framework for Institutionalizing Safety-by-Design	Sections 1, 5 Appendixes A,B,H,K,J	Institutionalization
B. Identification and description of requirements and success criteria	Sections 2, 4 Appendixes C,D,F,I	Requirements definition Technology & methodology
C. Optioneering study - Design & construct-ion management with SBD process for DOE environment incl. International Safeguards	Section 3 Appendixes E,G	Design processes
D. Best practices and lessons learned review	Section 4.1, 4.6 Appendix H	Technology & methodology
E. Working with the IAEA	Sections 2.4, 3.3, 4.3 Appendixes D, F, G	Requirements, Design, Technology & methodology
F. Summary and path forward – Institutionalizing Safeguards-by-Design	Sections 5, 7	All Framework categories
G. Support AFCF Design Project	Section 3.1 Appendix D-3	Requirements definition
Additional Items performed by SBD Team	**Provided in Report**	**ISBD Framework Categories**
H. Preliminary study of NRC domestic regulations for potential integration of SBD	Section 3.4, 4.4 Appendixes D,K	Design, Technology & meth-odology, Institutionalization
I. Development of Generic SBD process for generic design and construction management	Section 6	Design, Technology & meth-odology, Institutionalization

In FY-08, the framework for ISBD has been developed as an integrated approach for designing international safeguards, national safeguards and physical security, and nonproliferation objectives, into a new nuclear facility while integrating with all other project disciplines, including safety. The SBD process is a high-level procedure that can be applied to the design of most parts of the fuel cycle including facilities for: conversion, enrichment, fuel fabrication, nuclear reactors, and recycling. The SBD process supports the growth of nuclear energy while reducing nuclear security risks and:

Provides improved safeguards, security and proliferation risk reduction, while reducing the life-cycle costs to the operator and regulatory agencies

Focuses on early identification of intrinsic design features

Can be used internationally as the basis for establishing a high global standard for nuclear facility design

Creates a culture change to ensure the treatment of safeguards as a vital partner in the design process by using "systems engineering" to develop optimum integration of operations, safety, safeguardability, protectability, and proliferation resistance into the facility design.

The ISBD framework:

Directly supports the goals of the NNSA, NGSI

Supports the development of a "Safeguards Design Basis" similar to the "Safety Design Basis" used at nuclear reactors in the United States

Will facilitate various IAEA goals and objectives, such as:

Enhancing safeguardability in new nuclear facilities

Reducing the time and cost for the inspectors' physical presence at facilities

Incorporating process monitoring into the safeguarding of nuclear facilities

- Sharing equipment and instrumentation between the operator and the IAEA.

A fundamental component of the ISBD framework is the creation of a safeguards team using SBD during the initiation/pre-conceptual phase of the project to guide the project team in the integration of proliferation resistance, safeguards and security into the design, construction, readiness review, and startup of new nuclear facilities. The focus of the SBD process is that safeguards design activities be initiated in the earlier phase of the design process so the impact of safeguards requirements on facility alternatives analysis can be effectively evaluated during the conceptual design phase. The structured SBD process requires formal communication of safeguards issues and challenges to the regulator at each stage in the project. This timely identification and communication improves design integration and permits phased, cost-effective issue resolution. Because the proposed SBD process has a formal interface with the overall project risk management process and requires formal communication of risks and management strategies to the regulator, it has the potential to decrease the cost and schedule uncertainties associated with meeting safeguards requirements. The SBD process provides formal mechanisms to incorporate safeguards requirements in the structured systems engineering process for the facility design. Because the SBD process mandates early formation of a safeguards design team and early initiation of safeguards design activities, this enables safeguards input to the systems engineering evaluation of major design alternatives. This increases the likelihood that desirable intrinsic features will be incorporated in the design.

The SBD process developed in the study for DOE regulatory environment and international safeguards is expected to be readily adaptable for regulation by the NRC and with safeguards oversight by the IAEA even though the study was performed using DOE directives as a basis. The SBD process for DOE environment is compatible with the project phases and critical decision requirements identified in DOE O 413.3A (program management for acquisition of capital assets) and analogous to the approach established in DOE-STD-1189-2008 (integration of safety into the design process), which has been accepted in the safety arena. This latter approach is being implemented in current pilot projects, and the lessons learned from the DOE-STD-1189-2008 implementation can be incorporated into the SBD process. The SBD process builds on the guidance offered in DOE G 413.3-3 (Safeguards and Security for Program Management) and increases the specificity and the emphasis on early integration of safeguards design.

Critical Enablers for Safeguards-by-Design Process

- Strong organizational commitment to success (includes the top level management)
- Project manager is properly 'incentivized' and equipped (trained in Safeguards-by-Design process, project management, conflict management)
- SBD Team Leader is qualified, empowered and supported by the project management team
- Formal performance requirements and success criteria are in place for all SBD features of interest
- Full legal basis is in place to require support for SBD
- IAEA, project team and 'intermediaries' have a mutually agreed, unambiguous 'project plan', and follow this through in a timely fashion
- Historical stumbling blocks have been identified, recognized, and effectively dealt with:
  - Terminology
  - Project members are incentivized to achieve cross-functional solutions (as opposed to parochial objectives)
  - Clearance levels of project team (for classified design features …)
  - Intellectual property

Flowcharts have been developed to formalize the interaction of SBD within the overall facility design process and define new deliverables akin to safety reports, which assist the project director in ensuring safeguards requirements are met and allows the customer to provide formal advice of acceptability. Further requirements, criteria, and analysis techniques, e.g., for assessment of proliferation resistance, are recommended to achieve full benefit of SBD and ISBD. The SBD process identifies interaction points and deliverables required within the IAEA process affecting the U.S. facility design and construction. These enable the IAEA to increase the effectiveness of facilities' safeguards and fully integrate their systems into the design of facilities because it is important, at the key interaction points, that the IAEA offers timely input. The inclusion of International Safeguards experts as "project partners" in the SBD process is an important requirement for the successful implementation of the SBD process.

Several best practices and lessons learned, which have previously provided challenges to incorporating safeguards into the design and operation of facilities, have been studied and summarized. These confirm the benefits of early integration of safeguards within design and provide a historical context for understanding successes and failures of earlier integration.

A brief review of NRC processes for fuel facility licensing and commercial licensing status has been performed to examine potential translation of the SBD process to commercial facility regulation. This report identifies three potential routes for the introduction of SBD to the NRC arena.

5.2 Future Work Options under ISBD Framework

There are many options for work under the ISBD framework toward achieving a new global standard. The main proposals are summarized under the four ISBD categories.

5.2.1 Institutionalization

The ISBD framework directly supports the goals of the NNSA NGSI in its international safeguards aim of establishing a new global standard for effective application of SBD. A strategy is needed to transfer the ISBD framework and SBD process into international safeguards activities to promote efficient interaction by the IAEA with NNSA and DOE. Activities potentially include participation in drafting an IAEA technical document (TECDOC), developing an IAEA training course, and implementing SBD methodology on a project with IAEA safeguards oversight.

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

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

Sponsor review has started and is likely to continue depending on ISBD deliverables. Wider stakeholder review is planned. The list of stakeholders includes the NNSA; DOE Offices of Nuclear Energy, and Health, Safety and Security; Department of State; the DOE-STD-1189-2008 project team; projects Y-12 at Oak Ridge and Idaho Waste Treatment Project; facility design and construction managers and users of DOE O 413.3A; design team members of related disciplines (e.g., safety); and various subject matter experts. An expert group provided by the Energy Facilities Contractor Group drafted DOE STD-1189-2208. The Defense Nuclear Facilities Safety Board has a statutory role concerning safety of DOE facilities. NNSA and Department of State have primary positions in the implementation of the VOA and AP with the IAEA (DOE M 142.2-1).

A strategy is needed to apply the SBD process to design of commercial facilities. Uranium enrichment facilities may be the most safeguards-significant new commercial facilities in the near term in the United States. Two such facilities are under construction and two more NRC applications are expected—LES National Enrichment Facility gas centrifuge plant in New Mexico, USEC American Centrifuge Plant in Ohio, GE-H planning an application for a full-scale laser (SILEX) uranium enrichment facility in North Carolina, and AREVA planning a gas centrifuge enrichment plant in Idaho (see Appendix K). AREVA has announced its intent to proceed with a recycling facility in the United States. NRC has already issued the construction license for the MFFF and the licensing of operation is under review. The MFFF project team may be willing to review the SBD process. There are potential commercial deployment facilities such as the consolidated fuel treatment center. The SBD process should

be applied to actual facility projects to improve methodology, staff familiarization, and demonstrate benefits for stakeholders.

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

5.2.2 Requirements Definition

The development of updated safeguards regulatory requirements is essential. For the U.S., DOE directives, NRC regulations and CFRs predominate for the federal and commercial sectors, see Appendix D. The developed set should include complete international requirements, because these are sometimes sparse and lacking authority and will be needed under the AP. Acceptance criteria or other procedures are necessary to reconcile design, predicted performance and requirements. This report provides preliminary performance requirements and safeguards design guiding principles and extensively surveys relevant regulatory directives that form an important part of the prescriptive requirements. The proposed performance requirements are high-level and qualitative. Increased definition is needed to match the more tightly specified directives forming the prescriptive requirements for facility design. Further requirements, criteria and analysis techniques (e.g., for proliferation resistance) may be required for full implementation of SBD and ISBD. Some facility-specific safeguards requirements are likely to be agreed to between the owner/operator and the regulator.

For application of SBD within the DOE complex, new DOE implementing documents will need to be developed. Depending on DOE advice, many different approaches could be used to institutionalize the SBD process. A simple option exists for NNSA projects through addition of SBD requirements in the PRD. There could be additional directives, a DOE standard(s), and amendment of existing directives to invoke the use of new ones. An outline of a possible SBD directive, possibly a DOE standard, is included as Appendix J. A new DOE Order, Facility Safeguards, which integrates existing orders and new requirements, may be needed in an analogous way to DOE O 420.1B, Facility Safety, December 2005.

For an SBD standard, it is valuable to develop design guidelines. These are high-level principles to be followed in the design process. For example, for safeguardability, effective design seeks to eliminate or minimize process holdup of special nuclear material. Safeguards SSCs are preferred over administrative controls, and there should also be defense–in-depth with multiple independent barriers. For each relevant discipline within safeguards, a concise set of up–to-date and comprehensive guidelines should be developed.

The area of existing knowledge, e.g., standards, experience, know-how, and prior art, is important and often commercially protected by architect-engineer, construction, and operator organizations. Existing technology sets requirement expectations that may be conservative and derived from an era with lower safeguards standards. For example, the process flowsheet, or fuel-cycle selection, affects safeguardability, monitoring, and verification. It will be useful to publish, in high-level form, relevant prior art for various facility types, identifying both facility and system design features to enhance safeguardability and protectability, and catalog best safeguards practices. This covers batch item and bulk fissile material processing facilities including enrichment, reprocessing, conversion, fuel fabrication, and nuclear reactors (especially Advanced CANDU Reactor [ACR] and NGNP), storage, and transport.

5.2.3 Design Processes

An updated set of NRC safeguards requirements applicable as derived from CFRs and other directives needs to be developed. This set should include as complete as possible international requirements and any gaps identified. The SBD process should be tailored to the NRC licensing environment including process flowcharts, supporting methodologies and new draft directives where necessary.

The SBD process developed in the optioneering study for DOE design and construction management should be developed by producing more detailed format and content guidance for various SBD process deliverables, such as the Safeguards Effectiveness Report, Vulnerability Assessment Report, Cyber Security Plan, MC&A Process Analysis, and Proliferation Barrier Analysis, at each stage of the design process. Work would also include developing guidance for application of the graded approach to these documents and the overall SBD process. There is a need to elaborate and finalize a lower level, more detailed methodology of how to integrate the SBD Team into the DOE design process. This methodology should potentially include the steps of 30%, 60%, 90%, and 100% completion of design work within each design phase, defined participation in design reviews (e.g., DOE G 413.3-9, 9-23-08, Project Review Guide for Capital Asset Projects). The development of this detailed approach will assist the team in identifying the optimal mechanisms for integrating SBD into the facility design process. The overall process is considered to be applicable to a wide range of DOE fuel cycle facilities including potentially those for conversion, enrichment, fuel fabrication, reactors, and recycling.

The benefits and costs of opportunities for SBD pilot testing should be assessed for application of the SBD approach in a current DOE nuclear facility acquisition projects—for example, Las Alamos National Laboratory Chemistry and Metallurgy Research Replacement Project, Pantex Weapons Surveillance Facility, Savannah River Site Pit Disassembly and Conversion Facility, Oak Ridge Y-12 Uranium Processing Facility, or Savannah River MFFF (NRC licensed). Ideally, the project should have an active design team so the ISBD project can conveniently ask questions about the example and be able to trust the answer. When working from reports concerning terminated projects, it is difficult to get the needed level of information and to be confident that the basis for design decisions is well understood. The pilot test would involve requirement document formulation, criteria and analysis exploration, evaluation of design against performance, effectiveness of interaction of SBD, and project teams, etc. The chosen element might well be a uranium enrichment facility, because two are under construction in the U.S. and two more license applications are expected by NRC in 2009.

5.2.4 Technology and Methodology

Work in FY 2008 has identified useful approaches, several of which may possibly be combined for best effect to promote adoption of an SBD process tailored to the commercial nuclear sector (see Appendix K). Detailed examination of NRC-regulatory practices and proposals for future approaches, such as enhanced risk-informed and performance-based methodologies for fuel cycle facilities, is needed to optimize the SBD process for the commercial sector. Assessment of recent Gen IV PR&PP methodologies, the approach used by the NRC to integrate safety into the design and operation of nuclear facilities (NUREG-1513, 2001), and the Integrated Proliferation Resistance Analysis process will strengthen SBD for application within the NRC-regulated sector. The SBD approach is expected to readily accommodate most new proliferation resistance requirements and evaluation methodologies. ISBD supports the development of a “Safeguards Design Basis” similar to the “Safety Design Basis” used at nuclear reactors in the United States.

The IAEA requirements, given in Section 2, provided a high-level summary of safeguards practice. Ultimately, it is envisioned that the development of "Safeguards Best Design Practices" guides could capture the established safeguards design practices and solutions that have been implemented to date to address these safeguards verification requirements. These "Best Practices" would catalog the specific requirement and manner in which the safeguards issue was addressed. Even though the implementation of international safeguards varies to some degree individually from facility to facility, the fundamental safeguards requirements, especially for nuclear facilities of a given type, remain the same. Beyond this, "Safeguards Best Design Practices" need to be developed for each major facility type, with a strong connection to the fundamental or referenced requirements. These would need to be on a level of detail consistent with existing regulations and design practices as codified for electrical, mechanical, fire, chemical, and nuclear safety. This would assist facility designers by having clear methods of how to systematically address the international safeguards requirements, which are a major part of institutionalizing SBD.

The DOE facility design, safeguards best practice (developing an unclassified [UCNI] design requirements document from the vulnerability assessment, see Section 4.7) may have great value where gas centrifuge technology is both highly classified and protected commercially. Regarding another best practice, successful and unsuccessful initiatives and concepts may be studied concerning the integration of many aspects or parts, comprising or affecting overall safeguards and security. The paper "Integrated Safeguards: A 1988 Perspective" (Carlson 1989) (see Appendix H) triggered review of a range of safeguards integration papers spanning three decades.

5.3 Path Forward Options

Further work is needed to achieve the goal of establishing a new global standard for Safeguards-by-Design for new nuclear facilities. The following options are grouped into three major headings – development, demonstration, and promotion. They cover more work than is possible in the near term and do not cover all work in the longer term. Selected options are presented in Section 7.2 as the recommended path forward.

5.3.1 Further Development of Safeguards-by-Design

As it took a decade to develop and formalize the process for Safety-In-Design, a reasonably ambitious target to accomplish the same level for SBD is the end of FY-12 using pilot studies with NRC/DOE requirements and with clear management direction and adequate support. Tasks include:

FY-09: Conduct stakeholder review of the SBD process. Stakeholders that will be included are interested parties in NNSA and DOE Office of Nuclear Energy and Office of Health, Safety, and Security the DOE-STD-1189-2008 project team; projects Y-12 at Oak Ridge National Laboratory and Idaho Waste Treatment Project at Idaho National Laboratory; facility design and construction project managers and users of DOE O 413.3A; design team members of related disciplines (e.g., safety), in addition to subject matter experts. Update the process as warranted.

FY-09: Translation of the SBD process to the NRC licensing environment including process flowcharts, supporting methodologies, and new draft directives where necessary.

FY-09: Develop an updated set of NRC safeguards requirements applicable as derived from CFRs and other directives. This set should include as complete as possible international requirements and any gaps identified. All requirements need appropriate acceptance criteria or other procedures to reconcile design, predicted performance, and requirements.

FY-09–FY-10: Conduct NRC pilot project. Select an NRC facility design project, especially one with an active design team, which could benefit from application of SBD, on a trial basis, and use the

experience to guide refinement of the process as needed. Elaborate and finalize more details to produce a lower level process. Possible projects include NGNP and consolidated fuel treatment center.

FY-09–FY-10: Develop design guidelines for SBD. Design guidelines are high-level principles to be followed in the design process. For example, for safeguardability one would seek to "eliminate or minimize process holdup of special nuclear material." For each relevant discipline, a concise set of up-to-date and comprehensive guidelines should be developed.

FY-09–FY-10: Collect and publish relevant prior art for each main facility type, identifying both facility and system design features that are desirable to enhance safeguardability and protectability as well as cataloging proven safeguards solutions (best safeguards practices):

FY-09: Enrichment (centrifuge and laser), reprocessing (aqueous and electrochemical)

FY-10: Conversion, fuel fabrication, power reactors (especially CANDU), storage, transport.

FY-09: Write SBD implementing documents for the DOE directive system. Depending on DOE preference, the implementation within DOE could take various forms.

FY-09–FY-10: Conduct DOE pilot project. Select a DOE facility design project, especially one with an active design team, which could benefit from application of SBD, on a trial basis to refine the process. Elaborate details to produce a lower level process. Attach to a DOE project implementing DOE-STD-1189-2008. Assess the benefits and costs for pilot testing of SBD in current DOE nuclear facility projects, e.g., Los Alamos National Laboratory, Chemistry and Metallurgy Research Replacement Project, Pantex Weapons Surveillance Facility, Savannah River Site Pit Disassembly and Conversion Facility, and Y-12 U Processing Facility.

5.3.2 Demonstration of Safeguards-by-Design

The SBD process should be applied to actual acquisition projects to not only familiarize people with the process, and tune and improve it, but also to demonstrate that the proper application of the approach does produce benefits to the stakeholders. The above DOE pilot project is an example. Other candidate tasks are:

FY-09: Translation of the SBD process to the NRC licensing environment.

FY-09 and beyond: Demonstration and participation in U.S. facility design and construction projects. Involvement should vary according to the specifics of the opportunity. Candidates are MFFF at Savannah River Site (review the SBD process), AREVA Gas Centrifuge Enrichment Plant, General Electric-Hitachi SILEX enrichment plant, and the NGNP (a high-temperature gas reactor).

5.3.3 Promote Safeguards-by-Design as the New International Standard

These activities will directly support NNSA NGSI and the IAEA need to more efficiently implement effective safeguards. Some will be performed in direct collaboration with the IAEA under their newly launched SBD program, which commenced in October 2008, with conduct of an international workshop to identify design features, policy, and process that enhance safeguardability.

FY-09 through FY-13: Support IAEA's 'Nuclear Facility Design' (SBD) initiative.

FY-09: Translation of the SBD process into a model framework for country X. This result could then serve as the candidate model for establishing a new global standard for SBD. This could be worked in context of the IAEA's own SBD project.

FY-09 and beyond: Support IAEA in developing an international training course for ISBD. This training could address both the regulatory structure that a state would need to institutionalize the SBD process

and the training a project manager would need to implement the SBD process effectively in separate courses. The feedback from course participants would provide insights valuable in developing an internationally useful and accepted standard on ISBD.

FY-09 and beyond: Increase domestic and international recognition for the ISBD framework and SBD process by means of publications and workshops, promote increased public awareness and acceptance of SBD as an important enabler for global growth of nuclear energy, with reduction of security risk.

FY-10 and beyond: Leverage the international outreach capabilities of NA-242, and their cooperation programs, to promote the SBD approach in states that are pursuing the nuclear option. This would be analogous to the current outreach effort supporting export controls.

Other activities include participation in an international demonstration project of SBD, and enabling activities with appropriate international professional organizations, e.g., American Society of Mechanical Engineers, International Standards Organization.

6. GENERIC PROCESS FOR SAFEGUARDS-BY-DESIGN

After the experience of integrating the SBD process with that for DOE design and construction management (see Section 3), the SBD team was in a good position to identify quickly the SBD essentials in the form of a basic generic process. This work has several benefits including recognizing principles, enabling the testing of processes by comparison, improving SBD team understanding, aiding the comprehension of others, and facilitating the use of SBD within other domestic and foreign regulatory environments.

6.1 Planning Phase

The key elements of the generic SBD process during the planning phase are:

Mandated participation of safeguards subject matter expert(s) in concept development.

Identification of facility safeguards categorization (e.g., Section 5 of INFCIRC 225) and associated requirements as early in concept development as practicable.

Based on safeguards categorization, identification of applicable international, national, and organizational safeguards requirements. Separation of prescriptive safeguards requirements (e.g., security areas, physical barriers, intrusion detection) and safeguards performance requirements (e.g., ability to contain adversaries with design basis threat capabilities, capability to detect loss of significant quantity of special nuclear material). Performance requirements include mandatory safeguards "goals."

Application of formal SBD process on a graded approach based on: (1) safeguards categorization and (2) methodology for measuring the safeguards effectiveness.

Prescriptive requirements provided to project systems engineering process to be incorporated in design.

Conceptual strategies developed for meeting performance requirements including: (1) use of "off-the-shelf" safeguards measures, (2) research and development needed to enhance existing measures/develop new measures, and (3) design changes to enhance protectability and safeguardability (intrinsic measures). Development of unclassified design requirements to implement conceptual strategies. Design requirements provided to project systems engineering process to be incorporated in design.

Analyses demonstrating, with the appropriate level of assurance, that the conceptual strategies will meet the safeguards performance requirements. (At this stage of the project, these analyses should make conservative assumptions related to uncertainties in the capabilities of safeguards measures and overall design.)

Safeguards "envelope" (set of intrinsic features and associated requirements relied on for meeting safeguards prescriptive and performance requirements) identified at appropriate level and limited configuration management imposed.

Preliminary assessment of project risk associated with conceptual strategies for meeting safeguards performance requirements, including risk mitigation strategies (e.g., research and development, design changes).

- Documentation of safeguards categorization, applicable requirements, conceptual strategies developed for meeting performance requirements, safeguards envelope, and project risk assessment.
- Formal approval of these SBD elements is part of approval of project plans authorizing the project to proceed to the next phase.

6.2 Conceptual and Final Design Phases

The key elements of the generic SBD process during the design phases are:

Mandated participation of safeguards subject matter experts in design development. Leadership in safeguards design and review of all changes affecting safeguards envelope.

Validation of safeguards categorization and applicable requirements as design matures.

Refinement of strategies for meeting safeguards performance requirements as design matures. Modification of associated design requirements based on refined strategies and maturing design. Associated refinement of safeguards envelope and continuing configuration management, which becomes more formal as the design matures. (The increasing formality for safeguards requirements and design envelope is consistent with overall increasing configuration management stringency imposed in later phases of projects.)

Refinement of the analyses demonstrating that the safeguards strategies will meet the safeguards performance requirements. The refinement of these analyses reflect the maturing design, the reduction of uncertainties associated with the capabilities of safeguards measures and the design details, and the corresponding ability to use more sophisticated analytical approaches. The use of risk-informed methods for assessing and mitigating vulnerabilities is preferred.

Refinement of assessment of project risk associated with conceptual strategies for meeting safeguards performance requirements, including refinement of risk mitigation strategies based on maturing design and results of research and development activities. Implementation of risk management strategies as required.

Continued systems engineering and design activities to meet prescriptive safeguards requirements and design requirements needed to implement strategies for meeting safeguards performance requirements.

Refined documentation of safeguards categorization, applicable requirements, safeguards strategies developed for meeting performance requirements, analyses demonstrating adequacy of the safeguards strategies, definition of the safeguards envelope, and project risk assessment.

For facilities potentially subject to IAEA safeguards (i.e., on the EFL), the designer should collaborate with the IAEA regarding the information in the IAEA DIQ as early as practicable during the design phase. The Facility Attachment also should be jointly negotiated and completed during this phase.

6.3 Construction Phase(s)

The key elements of the generic SBD process during the construction phase(s) are:

Mandated participation of safeguards subject matter experts in review of field and design changes affecting safeguards envelope.

Refinement of the analyses demonstrating that the safeguards strategies will meet the safeguards performance requirements. The refinement of these analyses reflects field design changes, the demonstrated capabilities of safeguards measures, and the detailed as-built configuration.

Initial and continuing systems engineering and quality assurance validation activities, including performance validation, to verify that as-built design meets safeguards requirements, as construction proceeds. Safeguards acceptance reviews and validation at the conclusion of construction prior to turnover of the facility/process for operation.

Development of plans, policies, and procedures to implement strategies for meeting safeguards performance requirements in operation, including minor strategy modifications to address operational constraints.

Implementation of project risk management strategies associated with meeting safeguards requirements, as required.

Refined documentation of safeguards categorization, applicable requirements, conceptual strategies developed for meeting performance requirements, analyses demonstrating adequacy of the safeguards strategies, definition of the safeguards envelop, project risk assessment, and safeguards validation activities. At the conclusion of the construction activities, this documentation also includes (1) the results of safeguards acceptance reviews and validation and (2) the commitment documents (e.g., security plans, material control and accountability plans) required for safeguards and security approval of facility operation.

For facilities subject to IAEA safeguards, IAEA design verification activities are commenced, and the delivery and installation of IAEA safeguards equipment is to be completed during this phase. At the completion of construction, all equipment necessary for implementation of IAEA safeguards is to be installed, tested, and accepted. DIV continues throughout the facility's operational lifetime.

6.4 Key Features of the Generalized SBD Process

In summary, the key features of the SBD process are:

Early involvement of safeguards in the design effort

Early identification of safeguards requirements and intrinsic features that will benefit the design

Closer collaboration of safeguards with the project design, leading to improved cost and schedule estimates

A straightforward and simple interaction plan between safeguards and the formal design process that identifies required activities and their timeline and provides detail and analyses at each phase of the design cycle

Flexibility to incorporate all regulatory requirements into the design of nuclear facilities.

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

6.5 Comparison of the Generic SBD Process with that Developed for the DOE Environment

DOE projects are required to do a vulnerability assessment and prepare a cybersecurity plan. The prescriptive vulnerability assessment addresses performance adequacy of the physical protection system. The cybersecurity plan has been incorporated in the SBD deliberations because of the close relationship between cybersecurity needs of the owner/operator and the IAEA need for its own secure data collection, archiving, interpretation, and communication systems. NRC does not require a document analogous to a vulnerability assessment and an integrated MC&A / Physical Protection analysis may be an alternative approach. In general, there is unlikely to be a unique 'best way' to integrate requirements and assessment methodologies so that flexibility and judgment in application of the generic SBD process is important. The optimal locations for SBD process steps can also vary depending on the design and construction pattern that is chosen for the project.

The generic SBD process, shown in this section, documents the process essentials in a generic design and construction environment. Some further work in this area may be worthwhile to examine a minimal set of baseline safeguards performance requirements, as seen within the physical protection, MC&A, and International Safeguard requirements of NNSA, DOE, NRC, and IAEA, together with those established by other nations (e.g., France, Japan, and UK). Within this basic requirement set, the minimal process steps for SBD and their optimal positions could be established. These SBD activities may then be integrated more easily within a generic project management sequence that might incorporate as many as a dozen hold points (critical decisions) or as few as one or two. This may bring increased flexibility to institutionalize SBD within the framework of any of these safeguards oversight regimes. It is possible that the recommended refinement of the generic process will take place during future work with the IAEA toward developing a global standard for SBD. Such work will raise the general level of knowledge and understanding, but it is not yet clear whether such refinement will actually bring advances in use as compared to that developed in the optioneering study through expert judgment and documented in this report.

The questions posed above do not address the optimal points, in the overall generic facility design and construction project, for their accomplishment. The SBD activities for the DOE process are overlaid where they seemed to make the most sense given that the DOE project management and design processes represent a single path divided into phases with internal design reiteration within each phase. However, the project management process for NRC-licensed facilities may be quite different. They may use design-build with parallel pseudo-independent path activities or some other quite different process with many more or fewer hold points (e.g., critical decisions).

7. CONCLUSIONS AND RECOMMENDED PATH FORWARD

The conclusions and recommended path forward developed from the work performed during FY-08 are listed below.

7.1 Conclusions

In FY 2008, the ISBD project successfully developed a strategy and process, the ISBD framework for formalizing the development and use of the SBD process. These support the NGSI and key IAEA safeguards objectives, and are intended to be useful internationally in establishing a high-level global standard for nuclear facility design.

The authors believe that the SBD process can be applied beneficially today, using existing requirements and methodologies. The results obtained will be improved as more of the SBD framework is put into place and the designer's methodological toolkit is expanded. The development of design principles, guidelines, and best practices will be useful near term additions.

The SBD process is unlikely to be applied in the absence of formal requirements, or compelling evidence of value. Neither exists today. Industry motivation to voluntarily embrace SBD will depend on demonstrated value.

The framework is a general approach to increase the effectiveness and efficiency of the safeguards design process as part of nuclear facility design, construction, and operation. It is expected to be readily adaptable to almost all regulatory, management, and engineering environments and applicable to a wide range of facilities; although much work remains to achieve a new global standard.

Project activities have been performed within four categories: (1) definition of requirements that the SBD process must meet, (2) development of SBD processes to be applied during design and construction, (3) development of supporting technologies and methodologies, and (4) mechanisms for institutionalizing SBD.

The framework includes a generic SBD process, which was developed from a study of SBD within the DOE regulatory environment. Flowcharts were prepared from the activities comprising the SBD process, which confirmed viability and the compatibility with the relevant DOE directives.

Key features of the SBD process include: initiation of safeguards design activities in the preconceptual planning phase, early incorporation of safeguards into the project requirements, early appointment of an SBD Team, participation in facility design options analysis in the conceptual design phase to identify and 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.

Modern design practices are increasingly front end loaded, and the possibility to significantly influence major design features, such as process selection and plant layout, largely ends with conceptual design. Therefore, SBD's principal focus must be on the early inclusion of requirements, and the early identification of beneficial design features.

There are presently no broadly agreed upon design standards or formal design requirements for proliferation risk reduction, other than the existing requirements for international safeguards. Achieving additional nonproliferation objectives will necessitate the development and institutionalization of additional design requirements.

There is a need for development of supporting methodologies for the modeling and assessment of proliferation risk and the safeguardability of nuclear facilities so that safeguards implementation can be more rigorously evaluated, and safeguards-driven changes to basic design options at the conceptual design stage may be given more serious consideration by the project management.

7.2 Recommended Path Forward

Two categories of recommendations are made. The first lays out a strategic path forward, and second, a short series of specific projects are proposed to best implement the strategy in the near term.

7.2.1 Recommended Path Forward Strategy

The following strategy is proposed to facilitate further development of the SBD framework in order to achieve the overarching objective of a new international standard for a design process. It directly supports objectives of the NGSI. The strategy is organized under major headings of further development, demonstration, and international promotion of the SBD approach.

Further Development of the SBD Process

Process for SBD in design and construction: Finalize the proposed SBD process within the DOE regulatory environment (Conduct stakeholder review and trade study, and revise, establish, and formalize firm requirements for application of SBD process within the DOE context.)

Technology and Methodology: 1) Continue to develop and exercise the methodology and analytical toolkit for safeguards design and analysis and 2) develop design principles, design guidelines, best practices and performance requirements.

Requirements Definition: Propose and gain experience with proposed updated safeguards design and/or performance requirements, including proliferation resistance.

Demonstration of the SBD Process

Conduct pilot application in a DOE project still in an early design phase.

Adapt the generic SBD process to the NRC environment.

Conduct pilot application in an NRC-regulated project still in an early design phase.

Promotion of New Global Standard

Complete development of the generic SBD process for international application.

Define and perform outreach activities, including publications, conferences, and international projects.

7.2.2 Recommended Near Term Projects

These projects were selected from the list in Section 5 as candidates for early and best effectiveness in deploying the path forward strategy.

Finalize the proposed SBD process within the DOE regulatory environment

Provide support for IAEA's SBD activities

Develop SBD relevant best practices, requirements, design guidelines, design principles

Develop SBD process for other safeguards environments, e.g., NRC and foreign country

Perform pilot application in a DOE or NRC project

Perform outreach activities—publications, conferences, international projects.

8. REFERENCES

10 CFR Part 75, Safeguards on Nuclear Material – Implementation of U.S./IAEA Agreement.

Bjornard, T. and Pasamehmetoglu, K., "SESAME - Advanced Modeling and Simulation Applied to Nuclear Nonproliferation and Safeguards," INMM 47th Annual Meeting, Nashville, Tennessee, June 2006.

Carlson R. L., Integrated Safeguards: A 1988 Perspective, J. Nuclear Materials Management, pp. 10-19, January 1989.

DOE Additional Protocol Web Site, https://www.ap.doe.gov

DOE G 413.3-3, Safeguards and Security for Program and Project Management, 11-15-07.

DOE G 413.3-9, Project Review Guide for Capital Asset Projects, 9-23-08

DOE M 142.2-1, Manual for Implementation of the Voluntary Offer Safeguards and Additional Protocol with the IAEA, Approved: 9-4-2008.

DOE M 413.3-1, Project Management for the Acquisition of Capital Assets, 03/28/2003.

DOE M 470.4-7, Safeguards and Security Program References, U.S. DEPARTMENT OF ENERGY, Office of Security and Safety Performance Assurance, 08-26-05.

DOE O 142.2A, Voluntary Offer Safeguards Agreement and Additional Protocol with the IAEA – NNSA, Approved: 12-15-06 (NA).

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

DOE O 420.1B, Facility Safety, 12/22/2005.

DOE O 425.1C, Startup and Restart of Nuclear Facilities, 03/13/2003.

DOE P 470.1, Integrated Safeguards & Security Management (ISSM) Policy, 5-08-01.

DOE O 470.3A, *Design Basis Threat Policy* (U), 11/29/2005.

DOE-STD-1189-2008, Integration Of Safety Into The Design Process, March 2008.

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

Durst P.C., Advanced Safeguards Approaches for New Reprocessing Facilities IAEA/JAEA Workshop – Tokai-mura, Japan, November, 2007.

Executive Order 13458, Implementation of the Protocol Additional to the Agreement Between the United States and the International Atomic Energy Agency for the Application of Safeguards in the United States of America, February 4, 2008

Front End Loading Myths and Misconceptions presented at ECC Conference 2003 (at http://www.ecc-conference.org/35/pdfs/Clerecuzio_Lammers.pdf.

Gen IV, Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems, The Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group, GIF/PRPPWG/2006/005, Revision 5, pp. 65-69, November 30, 2006.

Generation IV International Forum/PRPP Expert Group, "Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems, Revision 5," GIF/PRPPWG/2006/005, November 30, 2006, printed by the OECD Nuclear Energy Agency for the Generation IV International Forum.

Golay, M. W., Risk-informed Operational Decision Management (RIODM): Risk, Event Trees and Fault Trees, Fall 2005, Lecture 1, Massachusetts Institute of Technology, http://ocw.mit.edu/NR/rdonlyres/Nuclear-Engineering/22-38Fall-2005/59146701-17E5-442F-A9A8-559A20C198EC/0/sec1_1.pdf.

Health and Safety Executive (HSE, UK), Report of the investigation into the leak of dissolver product liquor at the Thermal Oxide Reprocessing Plant (THORP), Sellafield, notified to HSE on 20 April 2005, *www.hse.gov.uk/nuclear/thorpreport.pdf* , published February 2007.

IAEA: IAEA Safeguards Glossary – 2001 Edition, "Subsidiary Arrangements and Facility Attachments," Paragraph 1.26, and Chapter-3, "Safeguards Approaches, Concepts and Measures," Vienna, Austria, 2002.

IAEA, The Structure and Content of Agreements between the IAEA and States required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons, IAEA INFCIRC/153 (Corrected), Vienna, Austria, June 1972. *www.iaea.org/Publications/Documents/Infcircs/Others/infcirc153.pdf*

IAEA, Carlson, J., The safeguards revolution - where to from here?, on behalf of SAGSI (Standing Advisory Group on Safeguards Implementation), Paper presented to IAEA Safeguards Symposium, Vienna, 16-20 October 2006.

IAEA, Design Information Questionnaire, Form N-91, June 2005 *www.nrc.gov/reading-rm/doc-collections/forms/iaea_n91.pdf*.

IAEA, International Symposium on Nuclear Security; Safety, Security and Safeguards Interfaces (3S Concept) - determine how the 3S concept can best be implemented by the international community and as a result build confidence that nuclear energy is generated in a safe, secure and proliferation resistant manner. Vienna, Austria, 30 March–3 April, 2009. *http://www-pub.iaea.org/MTCD/Meetings/PDFplus/2009/cn166/cn166_Announcement.pdf*

IAEA Department of Safeguards, "Proliferation Resistance Fundamentals for Future Nuclear Energy Systems," STR-322, December 2002.

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

NFPA, The National Electrical Code (NEC), or NFPA 70.

NFPA, National Fires Codes 2008 Edition, 15 Volumes.

NNSA, National Nuclear Security Administration: Nonproliferation and International Security Assessment, Next Generation Safeguards Roadmap, Office of NA-24, 2008.

NNSA, National Nuclear Security Administration, Policy Letter BOP-50.004, 02-15-2008.

NRC, NUREG-1513, Integrated Safety Analysis (ISA) Guidance Document, 2001.

Pomeroy G., et al, "Approaches to Evaluation of Proliferation Resistance of Nuclear Energy Systems," 49th Annual Meeting of INMM, Nashville, TN, July 13-17, 2008

Safeguards Assurances Corporation (SAC): Explanatory Notes and Model Responses for (IAEA) Design Information Questionnaires, Provided by the Program for Technical Assistance to the IAEA Department of Safeguards form U.S. DOE, ISPO-24, ISPO Task C.9, May, 1979.

Schanfein, Mark, "Science and Technology Challenges for International Safeguards," LA-UR-08-04468, INMM Annual Meeting, July, 2008.

United Nations Security Council Resolution 1540, Adopted by Security Council at its 4956th meeting on April 28 2004S/RES/1540 (2004).

Wood H. G., Glaser A. and Kemp R. S., The gas centrifuge and nuclear weapons proliferation, Physics Today, Vol. 61, Issue 9, September 2008.

9. GLOSSARY

Consistency and clarity in definition is important to the success of Institutionalizing Safeguards-by-Design and so all relevant terms are defined in this glossary.

Acquisition; Program or Project Management. For acquisition programs and projects are acquisitions of capital assets, equal to or greater than $5 million, regardless of the funding source, that deliver a product, or capability, with a specified beginning and end, a stated cost, and expected performance objectives. They are directed, funded efforts whose purpose is to provide a useful, material capability in response to a validated mission or business need. An acquisition program may be facility construction, infrastructure repairs or modifications, system, production capability, remediated land, closed site, disposal effort, software development, information technology, space system, research capability, or other asset. Acquisition programs, as they relate to projects, are generally made up of multiple projects, related by a common mission, in which each project remains a useful segment and able to perform its intended function.

Additional Protocol (AP) (Protocol Additional to Safeguards Agreements). Agreements with the IAEA made by states that specify the additional authority necessary for the IAEA to fully implement its obligations under comprehensive safeguards agreements pursuant to the NPT. APs contain measures to improve the efficiency and strengthen the effectiveness of the IAEA safeguards system. The main features of the AP are the requirements that states provide:

Information beyond that required for nuclear materials accountancy, e.g., on nuclear fuel cycle-related research and development, specified manufacturing activities (e.g., centrifuge manufacture) and exports and imports of certain non-nuclear material and equipment

Extended access to the IAEA to check this reporting.

AP declarations comprise information provided to the IAEA in accordance with the AP, Articles 2 and 3.

Alternatives Analysis. When design requirements are established, alternatives (i.e., options) are analyzed to establish a process approach, and facility and equipment arrangements are determined. The configuration alternatives are evaluated against technical, safety, safeguards, cost, and schedule criteria. As design requirements are established for each alternative; engineering, safety, and safeguards personnel will begin to identify alternative facility layout and processing configurations.

Comprehensive Safeguards Agreements. Agreements made with the IAEA by non-nuclear weapon states (NNWS) to enable the application of safeguards on all source and special fissionable material in all peaceful nuclear activities, as required by the NPT. The model text for these agreements is published as IAEA document INFCIRC 153.

Conceptual Design. The concept for meeting a mission need. The conceptual design process requires a mission need as an input. Concepts for meeting the need are explored and alternatives considered arriving at the set of alternatives that are technically viable, affordable, and sustainable.

Critical Decision (CD). A formal determination made by the architect-engineer and designated official (Mission Need Statement) at a specific point in a project life cycle that allows the project to proceed. Critical decisions occur in the course of a project, for example, prior to commencement of conceptual design, commencement of execution, and prior to turnover. (DOE O 413.3A, 2006).

Cyber Security. The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, against loss of accountability for information and user actions, and against the denial of service to authorized users, including those measures necessary to protect against, detect, and counter such threats. (DOE M 470.4-7)

Cyber Security Plan. A plan to show how the facility cyber resources will be protected from outside threats. This will include beginning to complete the SP 800-53 documentation to request Certification and Accreditation of the facility cyber resources. This plan will be updated as necessary in all phases of the design process.

Design Basis Threat (DBT). The statement that describes threats that are postulated for the purpose of analyzing Safeguards and Security programs, systems, components, equipment, information, or material (see DOE O 470.3, *Design Basis Threat Policy (U)* [DOE M 470.4-7].)

Design Criteria. Those technical data and other project information identified during the project initiation and definition (conceptual design, and/or preliminary design phases). They define the project scope, construction features and requirements, and design parameters; applicable design codes, standards, and regulations; applicable health, safety, fire protection, safeguards, security, energy conservation, and quality assurance requirements; and other requirements. The project design criteria are normally consolidated into a document, which provides the technical base for any further design performed after the criteria are developed.

Design Information Questionnaire (DIQ). Under IAEA safeguards, this is defined as "information concerning nuclear material subject to safeguards under the agreement and the features of facilities relevant to safeguarding such material." Design information includes the facility description; the form, quantity, location, and flow of nuclear material being used; facility layout and containment features; and procedures for nuclear material accountancy and control. This information is used by the IAEA, *inter alia*: to design the facility safeguards approach, to determine material balance areas and select key measurement points and other strategic points, to develop the design information verification plan and to establish the essential equipment list. Design information should be provided by the state as early as possible before nuclear material is introduced into a new facility. Further, the state is to provide preliminary information on any new nuclear facility as soon as the decision is made to construct, or to authorize the construction of, the facility, and to provide further information on the safeguards relevant features of facility design early in the stages of project definition, preliminary design, construction, and commissioning. Facility design information is to be provided for any safeguards relevant to changes in operating conditions throughout the facility life cycle. The state is to provide design information on principal nuclear facilities to enable the IAEA to perform the design review at as early a stage as possible. Design information is submitted to the IAEA by the state using the IAEA DIQ.

Design Information Verification (DIV). Activities carried out by the IAEA at a facility to verify the correctness and completeness of the design information provided by the state. An initial DIV is performed on a newly built facility to confirm that the as-built facility is as declared. A DIV is performed periodically on existing facilities to confirm the continued validity of the design information and of the safeguards approach. The IAEA authority for performing a DIV is a continuing right throughout all phases of a facility's life cycle until the facility has been decommissioned for safeguards purposes.

Eligible Facility List. A listing of nuclear facilities provided by the U.S. under the Voluntary Offer Safeguards Agreement (VOA) made by the IAEA with nuclear weapons states. It provides the IAEA with a list of nuclear facilities agreed to be open to IAEA safeguards activities including inspections on all source or special fissionable material. The eligible facilities are not associated with activities with direct national security significance to the United States. In accordance with the Agreement, the U.S. may add or remove facilities from the list as it deems appropriate.

Extrinsic (Institutional). Adjective relating to the actions undertaken to impede proliferation, sabotage, or theft by states or other institutions. These actions may be institutional, legal, or operational in nature. The noun "measures" is popularly used in this context, e.g., "extrinsic measures" to enhance proliferation resistance. Such use is not to be confused with the differing PR&PP use of "Measures" as used by the Generation IV International Forum (Gen IV, 2006) to mean bases or standards of comparison. Because of the different use of the term measures, Gen IV PR&PP talks of intrinsic and extrinsic features. Examples of extrinsic features to combat proliferation are international laws, treaties, protocols, import/export agreements, and the application of international safeguards and verification activities (including any safeguards measurement equipment employed, e.g., use of seals, cameras, motion sensors, remote telemetry and radiation detectors). An example of extrinsic features for physical protection would be the deployment of a physical security force to protect nuclear material.

Facility Attachment. IAEA defines that under an INFCIRC/153-type safeguards agreement, the state and IAEA may be required to agree on Subsidiary Arrangements. Subsidiary Arrangements to safeguards agreements consist of a General Part, applicable to all common nuclear activities of the state concerned, and of a Facility Attachment, prepared for each facility in the state and describing arrangements specific for that facility. In cases where several facilities are located in the same building and/or share a common store or stores (e.g., for multiunit reactor facilities), one facility attachment may cover the whole facility group. Subsidiary Arrangements may also consist of an attachment for a location (or group of locations) outside facilities in the state that are defined as one material balance area.

Facility Safeguards Approach. Under IAEA international safeguards, this is defined as the approach selected for safeguards implementation at a specific facility, developed by adapting the model approach (where such exists) to account for actual conditions at the facility as compared with the reference plant. The provisions for implementing the facility safeguards approach are incorporated in the Subsidiary Arrangements.

Final Design. Completion of the design effort and production of all approved design documentation necessary to permit procurement, construction, testing, checkout, and turnover to proceed. Final design occurs between Critical Decision-2 and -3.

Fuel Cycle. The series of steps involved in supplying fuel for nuclear power reactors. It can include mining, milling, isotopic enrichment, fabrication of fuel elements, use in a reactor, chemical reprocessing to recover the fissionable material remaining in the spent fuel, reenrichment of the fuel material, refabrication into new fuel elements, and waste disposal.

Functional and Operational Requirements (see Requirements). A work-product deliverable, typically high-level, which specifies the full requirements for a project or facility in nontechnical language that the system owners or users can understand. It includes functional (qualitative steps), performance (quantitative measures) and interface requirements. Describes in detail what will be delivered by the project or facility. It is used to help develop a common understanding between the project or facility owner/user and the project team concerning owner/user requirements. This understanding forms the basis for estimating, planning, performing, and tracking the project's activities throughout the life cycle.

IAEA. The IAEA, based in Vienna, is an independent intergovernmental United Nations organization that serves as the global focal point for nuclear cooperation. The IAEA assists its member states in planning for and using nuclear science and technology for peaceful purposes. It develops nuclear safety standards and, based on these standards, promotes the achievement and maintenance of high levels of safety in applications of nuclear science. The IAEA also verifies, through its inspection system, that States comply with their commitments under the Non-Proliferation Treaty and other nonproliferation agreements to use nuclear material and facilities for peaceful purposes only.

Institutionalizing Safeguards-by-Design (ISBD). The implementation of a structured approach by which international and national safeguards, physical security, and nonproliferation objectives are fully integrated into the overall design process of a nuclear facility, especially from preconceptual planning through design, construction, operation, and retirement of the facility.

Integrated Project Team. An Integrated Project Team is a cross-functional group of individuals organized for the specific purpose of delivering a project to an external or internal customer.

Integrated Safeguards and Security Management (ISSM). A set of principles and a formal methodology to integrate safeguards and security into management and work practices. (Derived from DOE P 470.1)

International Safeguards. Under the Treaty on the Non-Proliferation of Nuclear Weapons (Nuclear Non-Proliferation Treaty), the verification measures imposed by the IAEA to prevent the diversion of nuclear material from peaceful uses to nuclear weapons or other nuclear explosive devices. (DOE M 470.4-7)

Intrinsic. Adjective relating to the inherent properties and physical or process design features of a nuclear energy facility, process, system, or component. An intrinsic feature is likely to be very difficult or impossible to alter, is therefore very robust and desirable, and the term may be applied both to proliferation resistance and to physical protection. Intrinsic proliferation resistance features impede diversion, undeclared material production and/or misuse of technology, while intrinsic physical protection features deter sabotage, theft, harm to personnel, and protect against espionage. The beneficial action of an intrinsic proliferation resistance property may be indirect, i.e., by enabling the application of a more cost-effective or robust extrinsic feature. An example of an intrinsic proliferation resistance feature would be such a high decay heat rate so as to render a material unusable for a weapon. The placement of a facility completely underground would be an example of an intrinsic physical protection feature.

Life-Cycle Cost. The sum total of the direct, indirect, recurring, nonrecurring, and other related costs incurred or estimated to be incurred in the design, development, production, operation, maintenance, support, and final disposition of a major system over its anticipated useful life span. Where system or project planning anticipates use of existing sites or facilities, restoration, and refurbishment costs should be included.

Material Control and Accountability (MC&A). Those parts of the safeguards program designed to provide information on, control of, and assurance of the presence of nuclear materials, including those systems necessary to establish and track nuclear material inventories, control access to and detect loss or diversion of nuclear material, and ensure the integrity of those systems and measures. (DOE M 470.4-7)

Mission Need Statement. A concise document that details a mission requirement the department cannot meet through nonmaterial method.

National Safeguards. A nation's integrated 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. (extension from DOE M 470.4-7, 2005)

Non-Proliferation Treaty (Treaty on the Non-Proliferation of Nuclear Weapons; NPT). Under the NPT, the nuclear weapon states (China, France, Russia, United Kingdom, and U.S.) undertake not to transfer to any recipient whatsoever nuclear weapons or any other nuclear explosive devices or control over them, and not to support manufacture or acquisition of such weapons or devices by any non-nuclear weapons states (NNWS) (Article I). NNWS party to the NPT undertake not to receive any nuclear weapons or other nuclear explosive devices, nor to accept assistance in this respect (Article II). The NNWS party to the NPT also undertakes to accept IAEA safeguards on all source and special fissionable

material in all their peaceful nuclear activities. This undertaking is set out in agreements to be signed with the IAEA, which are known as Comprehensive Safeguards Agreements. The NNWS undertake further to provide source and special fissionable material and relevant equipment to any other NNWS only if the material is covered by IAEA safeguards (Article III). The NPT does not affect the right of its parties to develop and use nuclear energy for peaceful purposes. All parties to the NPT undertake to facilitate and have the right to participate in the fullest possible exchange of equipment, materials, and information on peaceful uses of nuclear energy (Article IV). Each of the parties to the NPT undertake to pursue negotiations on effective measures relating to an early cessation of the nuclear arms race, to nuclear disarmament, and to general and complete disarmament under international control (Article VI). The NPT was opened for signature on July 1, 1968, and entered into force on March 5, 1970. At its 1995 Review and Extension Conference, it was agreed that the Treaty would continue in force indefinitely. Only three states (India, Israel, and Pakistan) have not signed the NPT.

Nuclear Security. The security of nuclear facilities and nuclear material against all threats, both those of proliferation by states, and of theft or sabotage by subnational adversaries.

Operations Readiness Review (ORR). This assesses the appropriateness of facility startup or restart and is required for the initial startup of a new Hazard Category 1, 2, or 3 nuclear facility and restart after DOE directed unplanned shutdown, after extended shutdown, after substantial process, system, or facility modifications of Hazard Categories 1 and 2 nuclear facilities, etc. DOE requires contractors to prepare and implement the following documents: startup/restart notification reports, plans of action, ORR implementation plans, and final reports. DOE line management prepares its plans of action and ensures the ORR team leaders prepare ORR implementation plans and final reports. The resolution of all findings from the ORRs must be documented and maintained with the plans of action, implementation plans, and final reports (DOE O 425.1C).

Physical Protection . The application of physical or technical methods designed to protect personnel; prevent or detect unauthorized access to facilities, material, and documents; protect against espionage, sabotage, damage, and theft; and respond to any such acts should they occur. (DOE M 470.4-7)

Preconceptual Design (Preconceptual Planning). Definition stage of a project where mission need is formulated and iteratively reviewed, project planning is performed, early budget estimates made and initial assessment of requirements made.

Program Requirements Document. DOE National Nuclear Security Administration (NNSA) requires the submission of a Program Requirements Document (PRD) for construction programs/projects being executed by NNSA. It translates the “need” in the Mission Need Statement into initial top-level requirements addressing such concerns as performance, supportability, physical and functional integration, human integration, security, test and evaluation, implementation and transition, quality assurance, and configuration management. Experience has shown that a formal process resulting in an agreed-upon definition of requirements for new systems, new capabilities, updates, or enhancements to systems is a prerequisite to proceeding to system/capability design and also that failure to do this, results in rework and unnecessary costs and delays in schedule (NNSA Policy Letter BOP-50.004, 02-15-2008).

Project. In general, a unique effort that supports a program mission, having defined start and end points, undertaken to create a product, facility, or system, and containing interdependent activities planned to meet a common objective or mission. A project is a basic building block in relation to a program that is individually planned, approved, and managed. A project is not constrained to any specific element of the budget structure (e.g., operating expense or plant and capital equipment). Construction, if required, is part of the total project. Authorized, and at least partially appropriated, projects will be divided into two categories, major system projects and other projects. Projects include planning and execution of construction, renovation, modification, environmental restoration, decontamination and decommissioning

efforts, and large capital equipment or technology development activities. Tasks that do not include the above elements, such as basic research, grants, ordinary repairs, maintenance of facilities, and operations, are not considered projects.

Proliferation Barriers. Those aspects of facility design or operation (both intrinsic features and extrinsic measures) that impede the diversion or undeclared production of nuclear material or misuse of technology by the host state seeking to acquire nuclear weapons or other nuclear explosive devices.

Proliferation Resistance (PR; or Proliferation Barriers). Those characteristics of a nuclear energy system, which impede the diversion or undeclared production of nuclear material or misuse of technology by the host state seeking to acquire nuclear weapons or other nuclear explosive devices. The IAEA does not define nor use this term.

Protectability. The ease with which efficient and effective physical protection measures can be implemented for a nuclear facility.

Requirement. A condition or capability needed by a facility owner or user to solve a problem or meet an objective. A condition or capability which must be met or possessed by the facility and/or its inputs and outputs to satisfy a contract, standard, specification, regulation or other formally imposed requirements.

Risk. Risk is the Expected Consequence Vector of System Operation. Event Risk ≡ Vector (Set) of Expected Consequences from an Event. Total Risk is the sum over all Possible Events of the Risks associated with each Event, respectively (Golay 2005).

In the project management field, a particular example of risk is that of the measure of the potential inability to achieve overall project objectives within defined cost, schedule, and technical constraints and has two components. (1) the probability/likelihood of failing to achieve a particular outcome, and (2) the consequences/impacts of failing to achieve that outcome.

Safeguards. The term used to denote National Safeguards, International Safeguards, and Proliferation Barriers, as appropriate throughout this report.

Safeguards (including International and IAEA Safeguards). An integrated 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 (DOE M 470.4-7, 08-26-05). Internationally, safeguards are measures to verify that civil nuclear materials are properly accounted for and are not diverted to undeclared uses. Safeguards are conducted by an independent agency to verify that commitments made by states under safeguards agreements are fulfilled. Verification agencies include the IAEA, Euratom, and the Agencia Brasileño Argentina de Contabilidad y Control de Materiales Nucleares. The measures include nuclear material accountancy, containment, and surveillance. For nuclear weapons states, the measures are applied under the Voluntary Offer Agreement and AP to enable IAEA to detect diversion of nuclear material and undeclared nuclear activities.

Safeguardability. The ease with which a system can be effectively and efficiently put under international safeguards. “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.

Safeguards and Security. Safeguards and Security refers to the parameters of physical security that are built into a facility concerning access control, intrusion alarms, construction of vaults, property protection features, Operational Security, and even architectural surety. Safeguards and Security requirements, when applicable, are an integral part of project planning and execution and should be addressed early in the initial phase of a project and along with safety, quality, and environmental protection, integrated throughout all project phases.

Safeguards-by-Design (SBD). A structured process by which international and national safeguards, physical security, and nonproliferation objectives are fully integrated into the overall design process of a nuclear facility, especially from preconceptual planning to final design of a nuclear facility.

Safeguards Design Strategy (SGDS). The SGDS is a tool to guide project design and safeguards documentation development planning, and to provide approving authorities sufficient information upon which to base decisions. Using the SBD process, it provides a single, integrated compilation of the safeguards policies, philosophies, major requirements, and goals for the project. This strategy will be revised and updated as the project matures. The SGDS is structured to evolve into the information source needed for revising the Site Safeguards and Security Plan and the Nuclear Material Control and Accountability Plan.

Safeguards-by-Design Team. At the beginning of the project, the program/project manager establishes the Safeguards-by-Design-Team, with clearly defined roles and responsibilities, to support the project team in ensuring the integration of safeguards, security, and proliferation barriers throughout the design process, and to manage the preparation of relevant deliverables required to support each critical decision.

Safeguards System Design. Development of an integrated system of National Safeguards, International Safeguards, and Proliferation Barriers for nuclear facilities.

Safeguards Effectiveness Report (SGER). An updated SGER is prepared and submitted to DOE during each principal design stage, i.e., conceptual, preliminary and final design. Further updated versions may also be required prior to and during facility operations. For example, during conceptual design, the SGER comprises: requirements analysis; identification of key project interfaces; analysis of safeguards design concepts and justification of preferred alternative; safeguards design strategy; vulnerability assessment; initial safeguards risk and opportunities assessment; conceptual safeguards design; safeguards baseline cost estimates; and required technical studies to resolve risks and opportunities.

Safeguards Validation Report(s) (SGVR). These are prepared by DOE at key decision points including completion of conceptual, preliminary, and final design activities. They document the DOE reviews of the safeguards effectiveness reports and are prerequisites for moving from the definition phase to and through the execution phase. The DOE reviews the safeguards effectiveness reports against the safeguards design strategy and documents the reviews in the validation report to confirm that the safeguards positions adopted during conceptual, preliminary, and final design will meet the defined requirements, and constitute appropriately conservative bases to proceed.

Safety-in-Design. The process of identifying and incorporating appropriate structures, systems, and components (SSCs) and their associated safety functions and design criteria into the project design to provide adequate protection for workers and the public. (DOE-STD-1189-2008)

Site Safeguards and Security Plan. An official document required at facilities containing Category I special nuclear material or with credible rollup that describes the sitewide protection programs and evaluations of risk associated with DOE O 470.3, *Design Basis Threat Policy,* and identified facility targets. (DOE M 470.4-7)

Special Nuclear Material. Plutonium, uranium-233, uranium enriched in the isotope 235, and any other material which, pursuant to 42 U.S.C. 2071 (Section 51, as amended, of the Atomic Energy Act of 1954), has been determined to be special nuclear material, but does not include source material; it also includes any material artificially enriched by any of the foregoing, not including source material.
(DOE M 470.4-7)

Systems Engineering. 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. (DOE O 413.3A, Attachment 3)

Threat. This is defined as:

1. A person, group, or movement with intentions to use extant or attainable capabilities to undertake malevolent actions against departmental interests
2. The capability of an adversary coupled with his/her intentions to undertake any actions detrimental to the success of program activities or operations
3. Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. (DOE M 470.4-7).

Voluntary Offer Safeguards Agreements (VOA). Safeguards agreements made with the IAEA by the nuclear weapon states (i.e., China, France, Russia, United Kingdom, and U.S.). The NPT does not require the nuclear weapon states to conclude safeguards agreements, but they have all voluntarily offered parts or the whole of their civilian nuclear fuel cycle for the application of IAEA safeguards, in order to allay concerns expressed by NNWS that their nuclear industry could otherwise be at a commercial disadvantage.

Vulnerability. A weakness or system susceptibility that, if exploited, would cause an undesired result or event leading to loss or damage to national security. **Major Vulnerability.** A vulnerability which, if detected and exploited, could reasonably be expected to result in a successful attack causing serious damage to the national security. **Unspecified Major Vulnerability.** A major vulnerability, but specified in no greater detail than the specific security system (or one of its major components) when it occurs. (DOE M 470.4-7)

Vulnerability Assessment (or Analysis). A systematic evaluation process in which qualitative and quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a Safeguards & Security system to protect specific targets from specific adversaries and their acts. As nuclear facility design, construction, etc., proceeds the vulnerability assessments become more detailed with increased definition. Tools include security surveys, risk management, DBT, CARVER Method, Delphi Method, software vulnerability assessment tools, infrastructure modeling, etc. Psychology and brainstorming may be used to predict what the adversaries might do. An understanding of the security organization's goals, attributes, personnel, culture, and climate is important. (DOE M 470.4-7)

Vulnerability Assessment Report (VAR). A report associated with the safeguards and security management and planning process that describes the methodologies used in vulnerability analyses and the supporting information used, provides the results of vulnerability analyses and risk assessments, and establishes risk ratings. (DOE M 470.4-7)

Supporting sources used to develop this glossary are as follows:

1. DOE M 413.3-1, Project Management for the Acquisition of Capital Assets, Office of Management, Budget and Evaluation, pp. A-4-A16, March 28, 2003.
2. DOE G 420.1-1, Non-Reactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide, March 28, 2000.
3. DOE-STD-1189-2008, Integration of Safety into the Design Process, March 2008.
4. DOE-STD-3009-94, Preparation Guide for DOE Non-Reactor Nuclear Facility Documented Safety Analyses, July 1994, Change Notice No. 3, March 2006.
5. Management, Operations and Technical Controls Guidance, Cyber Security Program, DOE CIO Guidance CS-1, Attachment 4.

6. 10 CFR Part, 810, Assistance to Foreign Atomic Energy Activities, Energy, Chapter III--DOE, Subchapter I – Sales Regulation, July 2008.
7. 10 CFR Part 830, Nuclear Safety Management, includes Subpart B, Safety Basis Requirements, January 10, 2001.
8. 10 CFR part 835, Energy, Chapter III–DOE, Occupational Radiation Protection, revised final rule, June 2007.
9. 10 CFR Part 1017, Final rule, Identification and Protection of Unclassified Controlled Nuclear Information, effective December 8, 2008.
10. 10 CFR Part 70, Domestic Licensing of Special Nuclear Material.
11. 10 CFR Part 72, Licensing requirements for the independent storage of spent nuclear fuel and high-level radioactive waste, and reactor-related greater than Class C waste.
12. 10 CFR Part 73, Physical protection of plants and materials.
13. 10 CFR Part 74, Material control and accounting of special nuclear material.
14. 10 CFR Part 75, Safeguards on nuclear material-implementation of US/IAEA agreement.
15. Full-Text Glossary, U.S. Nuclear Regulatory Commission, http://www.nrc.gov/reading-rm/basic-ref/glossary/full-text.html, 2008.
16. Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems, The Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group of the Generation IV International Forum, GIF/PRPPWG/2006/005, Revision 5, pp. 65-69, November 30, 2006.
17. IAEA Safeguards Glossary, 2001 Edition, International Nuclear Verification Series No. 3, International Atomic Energy Agency, Vienna, 2002.

Institutionalizing Safeguards-by-Design: High-Level Framework

Volume 2 - Appendixes

Trond Bjornard PhD (INL), Joseph Alexander (INL), Robert Bean PhD (INL), Brian Castle (INL), Scott DeMuth PhD (LANL), Phillip Durst (INL consultant), Michael Ehinger (ORNL), Prof. Michael Golay PhD (MIT), Kevin Hase PhD (LANL), David Hebditch DPhil (INL), John Hockert PhD (PNNL consultant), Bruce Meppen (INL), James Morgan (ORNL consultant), and Jerry Phillips PhD PE (INL)

Idaho National Laboratory

INL/EXT-08-14777 - Revision 1

Cover photograph of uranium gas centrifuge enrichment plant (Schanfein, 2008). The design of modern uranium gas centrifuge enrichment plants will benefit from application of the Safeguards-by-Design process.

Contents

Appendix A

Potential Benefits of Safeguards-by-Design

Appendix A

A-1. REDUCED UNCERTAINTY IN PROJECT BUDGETS AND SCHEDULES

The SBD process takes full advantage of systems engineering through the early integration of safeguards, security, and nonproliferation considerations into the design process. It also adds additional resources to the design team, which enables a greater number of essential features to be considered earlier in the design process, which reduces the need for significant modifications to maturing facility designs. SBD breaks with the current design strategy that usually modifies mature facility designs or relies on add-on systems to bring the facility into compliance with safeguards regulations. This strategy introduces significant uncertainty in project budgets and schedules because this methodology increases the probability of unexpected complications associated with late design changes. These complications introduce uncertainties into the project budget and schedule early in the project's life, which limits their long term applicability.

A-2. INTERNATIONAL SAFEGUARDS

ISBD provides a framework for the integral consideration of international safeguards. There are formalized inclusion points that are built into the design process that provides the IAEA with opportunities to influence the facility design. This provides both the designer and the IAEA with the opportunity to increase the safeguardability of newly designed nuclear facilities, while designing in features that reduce the cost and time associated with the physical presence of IAEA inspectors at nuclear facilities. In addition, this affords the IAEA the opportunities to incorporate process monitoring capabilities into nuclear facilities and to enable the IAEA and the builder to share equipment and instrumentation should IAEA choose to do so. The broader potential benefits of the SBD process on international safeguards include producing facilities that can be more efficiently and effectively safeguarded.

A-3. INTEGRATION OF SAFEGUARDS, SECURITY, AND OTHER NONPROLIFERATION CONSIDERATIONS

The simple and effective strategy of formally incorporating the safeguards team early into the design process increases the effectiveness of the design team by enabling them, from the beginning, to focus on identifying intrinsic design features that cost effectively enhance and integrate safeguards, security, and nonproliferation considerations.

A-4. FEASIBILITY OF IMPLEMENTATION

The SBD process was designed to be adaptable to operate within any regulatory framework, and was applied as a study to the DOE acquisition process as established in DOE O 413.3A. The SBD process is compatible with the project phases and critical decision requirements identified in DOE O 413.3A and is analogous to the approach established in DOE STD-1189-2008. The study confirmed the feasibility of implementation with the context of a State System of Accounting and Controls (SSAC), in this case, that of DOE.

A-5. NRC

The logic of early involvement of Safeguards-by-Design, i.e., in the pre-conceptual planning phase, is very similar to that for cases of design of nuclear facilities for DOE. The possible, larger scale of handling and inventories of SNM for commercial facilities, as regulated by NRC, places even more importance on early integration of safeguards into design. Besides the potential greater cost impact due to scale, there may also be increased possibilities for novel design by incorporation of direct linkages between facilities such as fuel recycling and re-fabrication, which may exploit novel safeguards design. A major difference between DOE and NRC arenas lies in the differing approaches to design, i.e., where the former is the more prescriptive and the latter more risk informed and performance based in relation to design outcome. This brings the issue of how to influence early design of NRC-regulated nuclear facilities and this is discussed in Appendix K, Sections K-5 to K-7.

A recent development in the NRC domain is its publication No. 08-189, "NRC Issues Advanced Reactor Design Policy," dated October 14, 2008. One of the new suggestions is that designers should concurrently consider safety and security requirements while designing a facility, resulting in an overall security system that requires fewer human actions. One approach to meeting safety and security requirements with fewer human actions is to incorporate intrinsic features for safety, protectability, and safeguardability.

Appendix B

Institutionalizing Safeguards-by-Design, Project Work Plan, FY-08

Task ID: 24.243.2.6.9

Appendix B
Institutionalizing Safeguards by Design, Project Work Plan, FY 08
Task ID: 24.243.2.6.9

Office of International Regimes and Agreements
International Safeguards Policy and Treaty Implementation
(B&R NN4003010/2221195)
Work Plan FY08: 243.2.6.9

1). Task Title: Institutionalizing Safeguards by Design Task ID: 24.243.2.6.9 Rev 6: 01-26-08	2). Parent WBS in NAFD: 24.243.2.6: Safeguards Policy	3). Lab Participants: INL, LANL, ORNL. *(This is a joint project with NE Safeguards Campaign)*

4). Background and Objectives:

In the U.S., nuclear facility project design and construction requirements and the associated regulatory structure do not presently include a formal approach for integrating proliferation resistance and international safeguards requirements into the facility design phase. The same is true of national safeguards and security, which have tended to be incorporated into the facilities during the later stages of the project. The main objective of this project – which is sponsored by both NA-24 and the NE Safeguards Campaign (details defined below) - is to define an institutional approach to the design process that will provide a cost-effective, team approach for designing proliferation resistance, international safeguards and U.S. National Safeguards and Security into new nuclear facilities. It is essential that the approach must integrate intelligently and synergistically with safety and other relevant project disciplines, such as instrumentation and controls, process design, and so forth... Accordingly, Safeguards by Design is defined as 'the integration of safeguards (both international and national), physical protection and proliferation resistance as full and equal partners in the design process of a nuclear energy system or facility.'

The next step towards institutionalizing Safeguards by Design into the design process will take place during FY08 as this project completes the development of a comprehensive higher level framework for institutionalizing the design process. This framework will serve as the skeleton for other related, specific work performed in FY08, and it will also help to define, guide and influence the integration of future related efforts.

The work to be done will build on and dovetail with a similar, ongoing development process for incorporating Safety in Design (the ongoing development of DOE-STD-1189, presently in draft form). In the longer term the present project will inform a potential update to DOE Order 413.3A on Capital Project Management, and related guides, standards and orders. Commercial U.S. projects are regulated by the NRC, and the present DOE focused project is expected to provide a useful technical basis for consideration by the NRC. The institutionalized safeguards by design process will also include consideration of the interaction with the IAEA. Finally, this project will include the translation of the safeguards by design process to foreign countries, where there will be an analogous blend of national and international requirements to fulfill.

The project will be closely coordinated with the NE Safeguards Campaign and the application of international safeguards to the AFCF project. In FY08, INL will coordinate work under this task, with NA-243 funded participation by LANL and ORNL. INL is also coordinating the related project work performed under the NE Safeguards Campaign. Participation of other experts from INL, ORNL and PNNL is expected to be supported by the Safeguards Campaign.

5). Work Scope

Workscope for FY08
The focus of the project in FY08 is to develop and construct a strong, comprehensive higher level framework for institutionalizing safeguards by design into the design process. This framework will serve as the skeleton for specific work performed in FY08, and it will also help to define, guide and influence the integration of future related efforts.

In FY08 the integrated design process incorporating safeguards by design will be developed at a high level for the example of a DOE project. The translation of the process to other national contexts (NRC and the foreign 'model state') during this first year will be considered solely for purposes of informing the development process.

The interaction with the IAEA will be specifically taken into account, and the project will draw on experts with considerable IAEA inspector experience to lead this. Additionally, past applications of safeguards by design will be harvested and applied to the current development; this includes specifically the 1990's safeguards by design based upgrade to the INL Fuel Conditioning Facility (FCF, which houses the electrochemical reprocessing facility). This will be summarized in a chapter of the FY08 Summary Report which will specifically address both lessons learned and pitfalls and issues. Project workscope in future years is expected to include development of foreign model state applications and support.

A. Complete the High-Level Outline for Safeguards by Design

Safeguards by Design is defined as 'the integration of safeguards (both international and national), physical protection and proliferation resistance as full and equal partners in the design process of a nuclear energy system or facility.' During this first phase the project team will complete a high level outline defining the process to be followed to apply safeguards by design in the context of a nuclear facility design project. This framework will help to structure, guide and influence the integration of future related efforts.

B. Define Relevant Requirements and Success Criteria

A clear, definitive set of requirements to be applied to nuclear facility projects are needed, covering the disciplines proliferation resistance, international safeguards, national safeguards and security. Intimately related areas may also need to be specified, for example information security (part of national safeguards and security) also has a clear role in international safeguards (data authentication, and so forth). Accordingly, this phase of the project will assess, identify and propose relevant requirements to be applied for proliferation resistance, international safeguards, national safeguards and security, in their integration within a larger scope project. Also, a clear statement of the success criteria to be used to measure adequacy of measures to fulfill requirements is also required. While this will be very straight forward for those disciplines where there exists adequate and clear precedence and regulatory infrastructure, new ground must be plowed in other areas, such as proliferation resistance for example. This task does not include developing and proposing a new, quantitative definition of proliferation resistance, but will leverage design relevant work to date by both the IAEA/INPRO, as well as that of the Generation IV International Forum expert group on Proliferation Resistance and Physical Protection (PRPP). It is expected that this phase of the project with conclude with a number of recommendations

for further work.

C. Workshop - Stakeholder Review and Feedback

Stakeholders to the safeguards by design process will be given an opportunity to review the preliminary framework and provide feedback to the development process. It is planned to hold this workshop in May – after both the preliminary framework and requirements and success criteria have been developed – such that feedback can be incorporated into the balance of the work effort for FY08. A preliminary list of possible invitees would include appropriate staff from DOE-NA, DOE-NE, architect engineers (Washington Group, because of AFCF project involvement), national laboratories involved in nuclear facility design, DOE project management staff (e.g. AFCF, NGNP projects), GE, AREVA, URENCO (USA), U.S. representative to SAGSI, and nuclear utilities. The invitee list will be finalized after review with project sponsors.

D. Lessons Learned Review

A concerted effort will be made to identify past projects and experience in order to harvest and apply this experience to development of the safeguards by design process. This will include, among others, review of experience obtained in the upgrade of the FCF pyroprocessing facility, enrichment plant design experience, as well as other relevant experience that can be identified by the project team. The focus of the review will be specifically on identifying and capturing best practices, identifying sensitive and difficult issues, as well as pitfalls to be avoided. This experience, good and bad, will be codified as a chapter in the year end report, but will be completed in June so that the balance of the project can benefit from the conclusions.

E. Working with the IAEA

Because U.S. nuclear projects have typically been conducted without international safeguards, let alone active interaction with the IAEA during the design process, it will be particularly important to carefully examine aspects of the project that intersect with IAEA requirements and interests. Through participation by project team members who have had extensive experience in applying international safeguards at various facilities around the world, the safeguards by design activities associated with IAEA requirements and interaction will be carefully developed and documented. There are known difficulties to be addressed, including owner attitude about the apparent lack of benefit deriving from proactive cooperation with the IAEA. This will be the topic of a dedicated chapter in the year end report.

F. Summary and Path Forward: "Institutionalizing 'Safeguards by Design' into the Design Process"

This year end report will put some flesh on the skeleton defined in the outline for the high level framework. This document will identify and provide recommendations for areas for further development, and identify a clear path forward. This will include identification of needed methodology and support documents (e.g. guides, standards, orders, etc), as well as identification of regulatory issues that must be addressed. The document will include an outline of a proposed new DOE Standard that specifically addresses integration of safeguards by design into the design process. The document will emphasize projects within the context of DOE/IAEA requirements and interactions – specifically

including a chapter devoted to the IAEA as noted above - and will also clearly identify future work required to translate to NRC and 'model foreign state' applications.

G. Support AFCF Design Project

In both FY06 and FY07, NA-241 has supported the consideration of applying international safeguards to the AFCF and other nuclear facilities being developed by DOE-NE, via funding for individuals under the 'Safeguards by Design' project. Further progress on any of these facilities should include participation by members of this 'Institutionalizing Safeguards by Design' project team, for purposes of ensuring that the project planning, structure and execution reflect an integrated Safeguards by Design approach. Such projects provide a real and useful application environment that can help to inform and improve the design process.

Longer Term Workscope – FY09 and Beyond

The overarching longer term objective is to modernize the design and licensing process for nuclear facilities such that the cost-effective benefits of a risk-based, safeguards by design approach are achieved by all organizations involved in nuclear facility design, construction, licensing, operation and regulatory oversight. This will require updated, adapted or new processes and methodology for design, project management, and regulations, supported by appropriate documentation (guides, standards, manuals, orders, etc), and eventually also training. During FY08 this project will take a broad, high-level first step towards this objective, including a clearly defined map of the path forward that will define the workscope in future years.

The State level organizations to be considered are DOE and NRC in the United States, with this project focusing primarily on DOE. A generic 'model state' will be assumed for foreign applications, and it will benefit directly from translation of the US case. International safeguards will be assumed to apply for all cases, and the appropriate interaction with the IAEA will be included. In the longer term, regulatory adjustments will be needed in order to stimulate application of this modified approach to the design process as well as to administer and adjudicate effective implementation.

Office of International Regimes and Agreements
International Safeguards Policy and Treaty Implementation
(B&R NN4003010/2221195)
Work Plan FY08: 243.2.6.9

6). FY08 Budget ($000)

The DOE-NE Safeguards Campaign is funding workscope associated with state level safeguards and security. Team members are: Mr. Bruce Meppen (former Director, Safeguards and Security at ANL-W), Dr. Robert Bean (FY07 project team and safeguards), and Mr. Tim Leahy (former Director, Safety and NRC Licensing). This team is presently funded at the level of $135K for FY08 by the Safeguards Campaign.

NA-243 is funding project participation in activities as listed below. Items C, D, E, G and H have been added as a result of augmented funding by NA-243.

Activity	INL	LANL	ORNL				Total
A: High-level Outline							
B: Requirements Chapter							
C: Workshop							
D: Lessons Learned Review Chapter							
E: Working with IAEA Chapter							
F: Summary and Path Forward - Report							
G: Project Lead, Management, Reporting,Admin							
	200	150	125				*475*

Office of International Regimes and Agreements
International Safeguards Policy and Treaty Implementation
(B&R NN4003010/2221195)
Work Plan FY08: 243.2.6.9

7). Deliverables and Key Milestones:

	NA-243/241
Progress reports to NA-243	**Monthly**
Progress reports to NA-243, project coordination meetings, video- and teleconferences	**Quarterly**
A. High-level Outline	**February 28, 2008**
B. Requirements and Success Criteria Chapter	**April 30, 2008**
C. Intermediate Stakeholder Review	**May 31, 2008**
F. Summary Report, Path Forward	**September 30, 2008**

Note regarding schedule: Similar milestones are included in the NE Safeguards Campaign project planning system.

8). Project Team

NA-24 Funded Team Members
INL: Dr. Trond Bjornard (Project Lead)
LANL: Dr. Scott Demuth(International and National Safeguards, GNEP projects)
ORNL: Mr. Mike Ehinger (Reprocessing, Process Design, International Safeguards)
Mr. Jim Morgan (Enrichment Design and Operations, NRC Licensing)
Mr. Glen Hammond

HQ POC: George Pomeroy, Ed Wonder

NE Safeguards Campaign Funded Team Members
INL: Mr. Bruce Meppen, Mr. Joseph Alexander (U.S. Safeguards and Security, MPC&A)
INL: Dr. Robert Bean, Mr. Roger Haga, (FY07 project team, U.S. Safeguards)
INL: Mr. Jerry Phillips, Mr. Tim Leahy (Safety and NRC Licensing)
Others: TBD as funding permits (e.g. I&C, Information/Cyber security)

NE HQ POC: Mike Miller (LANL) Director, NE-Safeguards Campaign

Appendix C

Evolving Approach to Nuclear Safety

Appendix C
Evolving Approach to Nuclear Safety

C-1. INTRODUCTION

The United States civilian nuclear power enterprise is in its sixth decade of evolution. During that time its treatments of safety have evolved in ways offering parallel examples for the likely evolution of requirements for safeguards. This discussion summarizes that evolution and draws lessons for the potential future of the safeguards-by-design (SBD) enterprise, particularly concerning likely time and resource requirements needed to bring SBD to maturity. The Nuclear Regulatory Commission's (NRC) summary of this evolution is also available at http://www.nrc.gov/about-nrc/regulatory/risk-informed/history.html. The factors in the potential parallel structure of safety and safeguards are summarized in Table C-1.

Table C-1. Stages of evolution of nuclear safety and proliferation treatments.

Requirement	Safety	Proliferation
None	Before 1970	Before 1970
Back fitting of Required Systems	1970 – 1990	1990 - now
DBAs and GDCs used Internationally?	Currently	No
DBAs and GDCs used Domestically?	Currently	Yes
Scope for Significant Technological Improvements	Some	Large
Probabilistic Risk Assessment Used?	Currently	No

C-2. INITIAL TREATMENTS OF NUCLEAR SAFETY

The initial nuclear power reactors were derived from naval propulsion systems (light water reactors [LWRs]), and had available the experience gained with design and operation of the Manhattan Project reactors and the early Idaho test reactors. LWRs were used because the marginal costs of selecting them were much lower than with other technologies, for which the costs of initial development and delays would have to be incurred in addition to those of deployment. However, despite these advantages these reactors were designed in the absence of mature codified literature of good probabilistic risk assessment and performance requirements. Rather there was heavy reliance upon the common sense and experience of the Atomic Energy Commission staff and reactor designers.

C-3. BACK FITTING OF SAFETY SYSTEMS

The earliest power reactors had frontline and backup power control capabilities and frontline cooling systems for purposes of maintaining fuel integrity (e.g., the Indian Point 1 plant had no emergency core cooling system). All LWR plants had containment structures. Later, upon reflection, came recognition of the need for redundant systems performing critical safety functions.

C-3.1 Design Basis Accidents and General Design Criteria

This was followed by formulation for LWRs of general design criteria (GDCs) and design basis accidents (DBAs). These formulations were facilitated by the prior existence of LWR example plants that could be used to provide a framework for iterations of general principles, followed by applications as tests of feasibility, followed by refinement of the general principles, etc. This is important, because formulation

of GDCs and DBAs is much more difficult when attempted abstractly in the absence of examples upon which their probabilistic risk assessment may be tested critically and lessons derived.

C-3.2 LWR Technology Lock-in

The result of the head start given to LWR technologies is that their safety requirements quickly came to be defined in much greater detail than with other power reactor technologies. Inadvertently this situation then created incentive for preferring LWRs as subsequent power generation technology selections were made. This positive feedback system has resulted in LWRs being the dominant nuclear power technology in use worldwide, a position that appears unlikely to change soon.

C-4. PROBABILISTIC RISK ASSESSMENT

In the early 1970s larger capacity (e.g., 1200 MWe) power reactors began to be introduced, and political opposition to use of nuclear power hardened considerably. Much of this opposition focused upon claims that the planned power plants would be too unsafe. The discussion of such claims was made difficult by the absence of analyses quantifying the level of risk associated with nuclear power, in specific instances and generally. In order to resolve this debate, in 1972 the Atomic Energy Commission (AEC) initiated the Reactor Safety Study (RSS). In 1975 it produced the first large-scale probabilistic risk assessment (PRA), variously referred to as the RSS Report, WASH-1400 and the "Rasmussen" Report after the MIT Professor Norman Rasmussen, who was its principal architect.

In it the risks of a vector of potential power reactor accident consequences were estimated for a fleet of 100 reactors operating in the United States – a fleet much like that operating today. To oversimplify the report indicated that expected risks of prompt and latent fatalities due to power reactor operations were typically about two orders of magnitude lower than those due, respectively, from all accidents and cancers. The uncertainties associated with these results were not quantified explicitly, but the report included approximate estimates of the magnitudes of error factors (typically a factor of three, high or low) that could be applied to the mean results.

Proponents of nuclear power cheered the report, and opponents demonized it, largely according to the degree that the absolute results supported their respective positions. Both sets of pressure groups largely ignored the value of the report in demonstrating the use of probabilistic risk assessment for systematic identification of system vulnerabilities and in guiding the use of resources for reducing them. In practice these uses have come to be appreciated as the greatest benefits provided by probabilistic risk assessments, not the absolute quantifications that they produce. Rather, the political controversy provoked by the uses to which the reports results were put led to critiques of it, and ultimately to repudiation in January 1979 of the report's methods and results by the AEC's successor, the NRC. Its use in supporting important safety-related decisions was greatly inhibited until 1994 when the NRC issued its PRA Policy Statement. This statement rehabilitated the use of probabilistic risk assessment within the NRC, and recognized its place as a legitimate tool (in addition to deterministic analyses, tests and expert judgments) in supporting safety regulatory decisions. During the intervening 15 years probabilistic risk assessment was used to provide background information concerning generic safety questions, but not to support specific decisions. The NRC also used it in background to gain better understandings of generic safety questions. In effect the probabilistic risk assessment technique was tolerated and used where it had obvious benefit, but it was not legitimized.

C-4.1 Development of Probabilistic Risk Assessment and the NASA Experience

The probabilistic risk assessment technique was not developed for evaluation of nuclear power safety. Rather its foundations were developed in operations research during World War II in work focused upon

improvements in resource utilization and operational availability, with later applications in telecommunications. However, the probabilistic risk assessment version of reliability analysis was first developed in aerospace applications, but it did not flourish there as the messenger was rejected when the evaluated risks of such systems were unacceptably high from the perspectives of system designers and managers. This was starkly revealed following the 1986 Challenger space shuttle accident that killed all personnel aboard the craft. It emerged in Congressional hearings about the accident that the National Aeronautics and Space Administration (NASA) had discontinued use of probabilistic risk assessment using the rationale that it must necessarily be flawed when it persistently returned estimates of high risks. Rather, the common wisdom of the time was that the risks of space shuttle travel were low enough to justify the passenger voyages of civilians and Congressmen that had occurred prior to 1986.

That the probabilistic risk assessment technique would routinely reveal the systematic structural weaknesses that led to the accident was so embarrassing to NASA that use of the technique was then reinstated. Even then, 20 years and an additional space shuttle loss (with all hands aboard) passed before NASA was willing to state publicly the expected probability of a shuttle loss accident. Their published value is approximately 1/170, which is consistent with the observed frequency of such losses and much higher than prior beliefs. This experience illustrates the resistance to introduction faced by the probabilistic risk assessment technique. It is an example of the general willingness of individuals to reject information that conflicts with their desires—a common phenomenon, but concerning probabilistic risk assessment a strong barrier to introduction of a new technique for understanding the implications of complex systems.

C-4.2 Introduction of probabilistic Risk Assessment

This experience may prove to be important concerning introduction of the probabilistic risk assessment technique within the SBD framework. The reason for this concern is that it was repeated in the area of nuclear safety. The main factor that ultimately supported the resurrection of probabilistic risk assessment concerning safety was occurrence of the core damage accident at the Three Mile Island (TMI) unit two reactor. It occurred in March 1979, about two months following repudiation by the NRC of the RSS results and of the probabilistic risk assessment technique. This accident had been foretold in the RSS in an approximate form and was in a class of power plant safety vulnerabilities not identified by alternative safety analysis techniques. Even so, this vindication of the technique still required a long time before it was allowed to be used without taint in supporting decisions. This interregnum can be explained by the need for a long time before social attitudes and preferences would change enough to allow its use in a routine non-controversial fashion.

C-4.3 IPE and IPEEE

During the 1980s and 1990s probabilistic risk assessment continued to be used within the United States nuclear power enterprise, but in the background. This was most important concerning the requirement by the NRC of the Individual Plant Evaluation (IPE) and IPE External Events programs (IPEEE). In these efforts each licensed reactor was required to be subjected to at least an approximate probabilistic risk assessment. The scopes of these analyses varied according to the preferences of the licensees, at one extreme addressing only the expected implications within the reactor of internal initiating events and at the other including the effects of external initiating events (especially earthquakes) within a zone surrounding the power plant, quantifying the effects of knowledge-related uncertainties and performing system sensitivity and risk importance analyses. In each case the goal was to identify risk-important plant modifications that might be needed, but the search was not vigorous.

C-4.4 NUREG 1150

The most important successor study to the RSS was the NUREG 1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants" in 1990. It extended the treatment of uncertainties very thoroughly, and made extensive use of expert knowledge in instances where objective quantified data were unavailable. It examined the risks of a set of five power plants, typical of those used in the United States, and was important in revealing risk differences of the various types of reactors and containment systems in use. The results of NUREG 1150 also reflected a trend typical of probabilistic risk assessments performed over the three decades during which most have been created: As system understanding and operational probabilistic risk assessments improve (in part driven by use of probabilistic risk assessment results in managing operations) the estimated risks of nuclear power plants have declined steadily.

The NRC's Quantitative safety goals: In 1988, at the direction of the Congress, the NRC promulgated its Quantitative safety goals, stating explicitly acceptable levels of nuclear power plant prompt and latent fatality risks to be a factor of 0.001 of the risks of accidental or cancer-related fatality, respectively, from all sources for a person living within a defined zone around a nuclear power plant. These risks are evaluated using the probabilistic risk assessment technique. However, they are not regulatory requirements. Rather they are factors to be considered, among others, in evaluating whether a nuclear power plant poses undue risks to its neighbors. Use of the safety goals has been an important influence in guiding the use of resources in improving nuclear power plant safety.

C-4.5 Probabilistic Risk Assessment Policy Statement and Regulatory Guide 1.174

The NRC's 1995 Probabilistic Risk Assessment policy statement, discussed previously, has opened the door wider for more direct use of probabilistic risk assessments in supporting regulatory decisions and processes. Among the more important uses was development of the Regulatory Guide 1.174 regulatory process governing proposed modifications to the configuration and operational procedures of a licensed nuclear power plant. Within this process probabilistic risk assessment has a role equal to those of deterministic engineering analyses, tests and expert judgment in evaluation of the acceptability of a proposal. It utilized risk-based acceptance criteria and provides implicit standards for treatments of uncertainty as acceptance limits are approached. It also permits occasional small increases in plant risks provided that they are within the range of the uncertainties of estimated performance.

C-4.6 The NRC's Maintenance Rule

The NRC's Maintenance rule was promulgated in 1996 for use in guiding negotiation between a licensee and the NRC of acceptable probabilistic risk assessments in maintaining a nuclear power plant adequately. Risk criteria and evaluations are used in deciding what maintenance procedures should be performed, the frequencies and remedial activities to be required should the desired performance results (from tests) not be obtained. A benefit of this approach has been to transfer to the licensee clear authority and responsibility for obtaining acceptable performance results.

C-4.7 Technology Neutral Risk Informed Licensing Process

The Technology neutral risk informed licensing process has been under development for more than two decades, and is not yet completed. It is the most parallel safety-related intellectual structure to what can be foreseen for risk-informed SBD. It uses probabilistically formulated system performance acceptance goals, supported by a graded approach in assigning resources for ensuring good performance as the system's expected performance approaches an acceptable limit. Its goals are to focus evaluation of a system upon its performance outcomes rather than the means used to achieve them and to include uncertainties in an explicitly clear fashion as elements in the evaluation. As with the risk-informed license

amendment system for an existing plant the toolkit of probabilistic risk assessment, deterministic analyses, tests and expert judgment are used in the assessment of system performance.

Its development remains unfinished mainly because the resources needed for its maturation into a routinely reliable evaluation method have not been applied at a sufficient level. There are no fundamental conceptual developments needing to be overcome, rather, the remaining work is concerned with demonstrating the practicality and providing examples of use of its methods, and working through the details of treatments of the many questions that must be confronted in an evaluation (e.g., common cause failures, human errors, use of expert judgment). This work is needed so that practitioners will be able to use its methods in a confidently reproducible fashion, based upon consensus concerning acceptable treatments of disparate safety questions.

There is no reason to expect this process of maturation not to be completed when the needed resources are applied, but performance of the needed developmental studies is essential for completion. This is also relevant to SBD, because the same process of maturation and resource application arises with it. This reality must be accepted and responded to if SBD is to become a feasible design and evaluation approach.

C-4.8 Contrast to Other Countries

Internationally probabilistic risk assessment applied to nuclear safety problems has not gained the level of acceptance found in the United States. It is used worldwide, but its influence is similar in most other countries to what had been found in the US prior to issuance of the NRC's 1994 PRA Policy Statement. Explanations for this situation likely include that the use of nuclear probabilistic risk assessment originated in the US, where it has always been influential, to the nuclear power industries of other countries being more protected from commercial competitive influences and perhaps to greater conservatism within the engineering professions. However, it is a factor to consider in anticipating what barriers might inhibit international acceptance of SBD.

C-4.9 Lessons from the Evolution of Risk Informed Nuclear Safety Regulation

The evolution of risk-informed nuclear safety regulation and its foundation upon probabilistic risk assessment have lessons relevant and useful for managing the maturation of the SBD process. In planning this process each of the factors listed below should be recognized and accommodated.

Among the most important lessons are the following:

- The acceptance of use of probabilistic risk assessment in various industries and settings has been a slow process, impeded by unfamiliarity with and complexity of the method, and sometimes by its role as bearer of unwelcome news.
- The great value of probabilistic risk assessment is in its ability to provide an integrated assessment of a system's performance, taking into account all factors that an analyst may consider to be important. This assessment can include the effects of uncertainties, sensitivities, and the importance of the various factors affecting the results provided.
- When used in an undisciplined fashion any modeling treatment can yield unreliable results (as with use of rosy inputs and assumptions). Only after performance of many similar analyses and comparison of their results and sensitivities has it been feasible for consensus to emerge concerning safety analyses. This experience has permitted creation of understanding of essential elements and treatments that should be expected in a high quality analysis, and has retarded use of probabilistic risk assessment in generating falsely optimistic results. It is essential to recognize that short cuts to reaching such a stage of understanding do not exist, either in safety or proliferation applications.

- Considerable investments are required for creation of the needed body of data, library of models and analytical tools and the cadre of seasoned analysts in order to support performance and cross examination of many analyses. Also, once created, these analytical assets must be sustained through consistent use, or they will atrophy.

The implications of these lessons for SBD are reasonably obvious, as its maturation appears likely to parallel that of the treatment of safety. Doubts that this maturation into a valuable treatment of proliferation problems is feasible are as unfounded as are those that it can occur easily.

C-5. REFERENCES

Reactor Safety Study (Report WASH-1400) US Atomic Energy Commission (1975).

Severe Accident Risks, An Assessment for Five United States Nuclear Power Plants (Report NUREG 1150) US Nuclear Regulatory Commission (1990).

PRA Policy Statement, (60 FR 42622) US Nuclear Regulatory Commission (1995).

Regulatory Guide 1.174 An Approach for Using Probabilistic Risk Assessments in Risk Informed Decisions on Plant Specific Changes to the Licensing Basis, US Nuclear Regulatory Commission (1997).

Appendix D

National and International Safeguards Requirements for the Nuclear Fuel Cycle

Appendix D
National and International Safeguards Requirements for the Nuclear Fuel Cycle

D-1. PHYSICAL PROTECTION

Volume 1, Section 2 summarized requirements for SBD. This appendix provides wider coverage and greater detail.

The objective of physical protection is to protect and control SNM and classified matter, as well as to protect unclassified sensitive matter, Government property, and the environment. Physical protection encompasses the entire physical security program at a facility including security equipment, procedures, protective forces, management and supervision, and the integration of these elements into a total system.

Physical Protection. The application of physical or technical methods designed to protect personnel; prevent or detect unauthorized access to facilities, material, and documents; protect against espionage, sabotage, damage, and theft; and respond to any such acts should they occur. (DOE Manual 470.4-7, 8-26-05).

Relevant DOE directives are now listed in Table D-1.

Table D-1. Directives relating to physical protection.

No.	Title
DOE O 413.3A	Program and Project Management for the Acquisition of Capital Assets (07/28/2006)
DOE G 413.3-3	Safeguards and Security for Program and Project Management (11/15/07)
DOE M 461.1-1 Chg 1	Packaging and Transfer of Materials of National Security Interest Manual (09/29/2000)
DOE O 461.1A	Packaging and Transfer or Transportation of Materials of National Security Interest (04/26/2004)
DOE P 470.1	Integrated Safeguards and Security Management Policy (05/08/2001)
DOE O 470.2B	Independent Oversight and performance Assurance Program (10/31/2002)
DOE O 470.3A	Design Basis Threat Policy (11/29/2005)
DOE M 470.4-1 Chg 1	Safeguards and Security Program Planning and Management (08/26/2005)
DOE M 470.4-2 Chg 1	Physical Protection (808/26/2005)
DOE M 470.4-2 Chg 1 Section B	Safeguards and Security Alarm Management and Control Systems (SAMACS) (08/26/05)
DOE M 470.4-3 Chg 1	Protective Force (08/26/2005)
DOE M 470.4-4 Chg 1	Information Security (08/26/2005)
DOE M 470.4-5	Personnel Security (08/26/2005)
DOE M 470.4-7	Safeguards and Security Program references (08/26/2005)
DOE O 470.4A	Safeguards and Security Program (05/25/2007)

The abstracts for these directives are provided as follows:

- DOE O 413.3A (Order, 07/28/2006), Program and Project Management for the Acquisition of Capital Assets

  The Order provides the DOE, including the National Nuclear Security Administration, project management direction for the acquisition of capital assets that are delivered on schedule, within budget, and fully capable of meeting mission performance and environmental safety and health standards.

- DOE G 413.3-3 (Guide, 11/15/07), Safeguards and Security for Program and Project Management

  Goal: To ensure that safeguards and security requirements are identified and integrated into a project early and that their implementation is assessed throughout the project life cycle. Establishing and integrating safeguards and security requirements early is necessary for project planning and cost estimating and to prevent project impacts that can be expected when safeguards and security requirements are identified late into the design process, construction, or as part of the operational readiness review. The integration of all requirements is critical to developing the best overall cost effective solution for the project.

  (Note on page I-2 of Guide: Alternative methods that are demonstrated to provide an equivalent or better level of protection are acceptable. DOE encourages its contractors to go beyond the minimum requirements and to pursue excellence in their programs.)

  Objectives:

  a. To integrate safeguards and security consideration into each acquisition management phase (initiation, definition, execution and transition/closeout)
  b. To define security project's features and functions as developed or required by the security program or security policy which minimized impact on operations
  c. To identify the function of the federal site security program representative who serves as security design point of contact for security features and is a member of the integrated project team (IPT) as appropriate during the entire project cycle
  d. To facilitate communication and interaction between the site security professionals, other integrated project teams, and the members of the project design team.

- DOE M 461.1-1 chg 1 (Manual, 09/29/2000), Packaging and Transfer of Materials of National Security Interest Manual

  This technical manual establishes requirements for operational safety controls for onsite operations and provides DOE technical safety requirements and policy objectives for development of an Onsite Packaging and Transfer Program, pursuant to DOE O 461.1A, Packaging and Transfer or Transportation of Material of National Security Interest.

- DOE O 461.1A (Order, 04/26/2004), Packaging and Transfer or Transportation of Materials of National Security Interest

  To establish requirements and responsibilities for offsite shipments of naval nuclear fuel elements, Category I and Category II special nuclear material, nuclear explosives, nuclear components, special assemblies, and other materials of national security interest.

- DOE P 470.1 (Policy, 05/08/2001), Integrated Safeguards and Security Management (ISSM) Policy

  The purpose of this policy is to formalize an Integrated Safeguards and Security Management framework. Safeguards and security management systems provide a formal organized process for planning, performing, assessing, and improving the secure conduct of work in accordance with

risk-based protection strategies. These systems are institutionalized through DOE directives and contracts.

- DOE O 470.2B (Order, 10/31/2002), Independent Oversight and Performance Assurance Program

  The Independent Oversight Program is designed to enhance the DOE safeguards and security; cyber security; emergency management; and environment, safety, and health programs by providing DOE and contractor managers, Congress, and other stakeholders with an independent evaluation of the adequacy of DOE policy and the effectiveness of line management performance in safeguards and security; cyber security; emergency management; environment, safety, and health; and other critical functions as directed by the Secretary.

- DOE O 470.3A (Order, 11/29/2005), Design Basis Threat Policy

  This document is classified.

- DOE M 470.4-1 Chg 1 (Manual, 08/26/2005), Safeguards and Security Program Planning and Management

  The manual established program planning and management requirements for the Departments Safeguards and Security.

- DOE M 470.4-2 Chg 1 (Manual, 808/26/2005), Physical Protection

  This manual establishes requirements for the physical protection of safeguards and security interests. Copies of Section B, Safeguards and Security Alarm Management System, which contains Unclassified Controlled Nuclear Information, and Appendix 1, Security Badge Specifications, which contains Official Use Only information, are only available, by request, from the program manager, protection Program operations.

  This order covers physical protection requirements for domestic DOE Sites:

  - Protection Planning
  - Protection of Nuclear Weapons and Special Nuclear Materials
  - Protection of Classified Matter
  - Radiological, Chemical, and Biological Sabotage Protection
  - Security Areas
  - Alarm Management and Control System
  - Protection of Security Systems Elements
  - Intrusion Detection and assessment Systems
  - Access Control and Entry/Exit Inspections
  - Barriers and Locks
  - Secure Storage
  - Communications
  - Maintenance
  - Posting Notices
  - DOE Badge Program

- DOE M 470.4-2 Chg1 Section B (Manual, 08/26/05), Safeguards and Security Alarm Management and Control Systems (SAMACS)

  The requirements for Safeguards and Security Alarm Management and Control Systems (SAMACS) used in the protection of Category I and II quantities of SNM and installed and operational after January 1, 2008, are contained in Section B of DOE M 470.4.2 Chg 1. The document contains

Unclassified Controlled Nuclear Information (UCNI) and can only be acquired through special request from DOE-HQ.

- DOE M 470.4-3 Chg 1 (Manual, 08/26/2005), Protective Force

  This manual establishes requirements for management and operation of the DOE Protective Force, establishes requirements for firearms operations and defines the firearms courses of fire.

- DOE M 470.4-4 Chg 1 (Manual, 08/26/2005), Information Security

  This manual establishes security requirements for the protection and control of information and matter required to be classified or controlled by statutes, regulations, or DOE directives.

- DOE M 470.4-5 (Manual, 08/26/2005), Personnel Security

  The manual establishes the overall objectives and requirements for the DOE Personnel Security Program.

- DOE M 470.4-7 (Manual, 08/26/2005), Safeguards and Security Program references

  This manual establishes definitions for terms related to the DOE Safeguards and Security Program and includes lists of references and acronyms/abbreviations applicable to Safeguards and Security Program directives.

- DOE O 470.4A (Order, 05/25/2007), Safeguards and Security Program

  The Order establishes roles and responsibilities for the DOE Safeguards and Security Program.

D-2. GENERALIZED SAFEGUARDS REQUIREMENTS FOR ALL REGULATING AGENCIES

The ISBD framework is presently primarily addressing DOE safeguards requirements with study of IAEA interactions but is expected to be extended to NRC regulation for commercial nuclear facilities. The classic safeguards requirements and their generalized categorization are shown in Figure D-1.

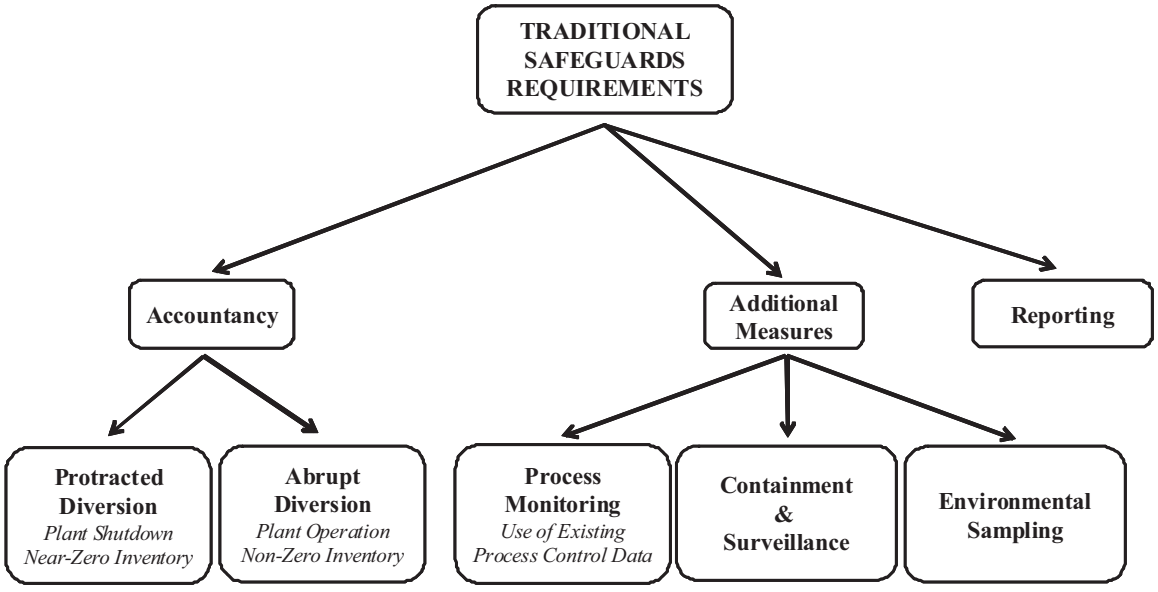


Figure D-1. Generalized safeguards requirements for all regulating agencies.

The abrupt diversion category is expanded and quantified in Figure D-2 for the three effective regulatory agencies.

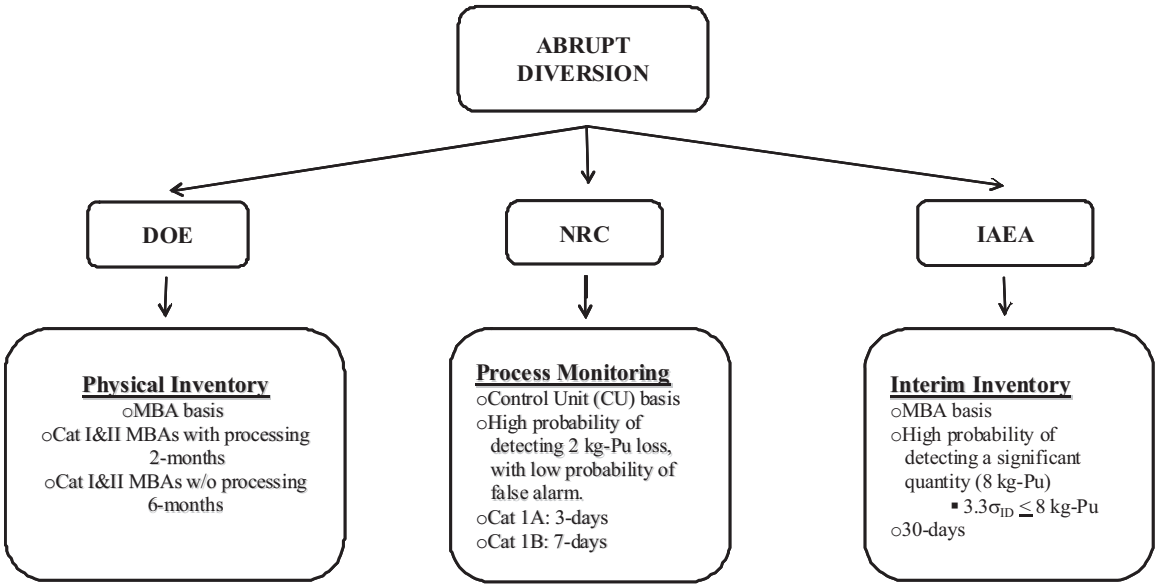


Figure D-2. Abrupt diversion accountancy requirements for each regulating agency

The protracted diversion category is expanded and quantified in Figure D-3 for the three effective regulatory agencies.

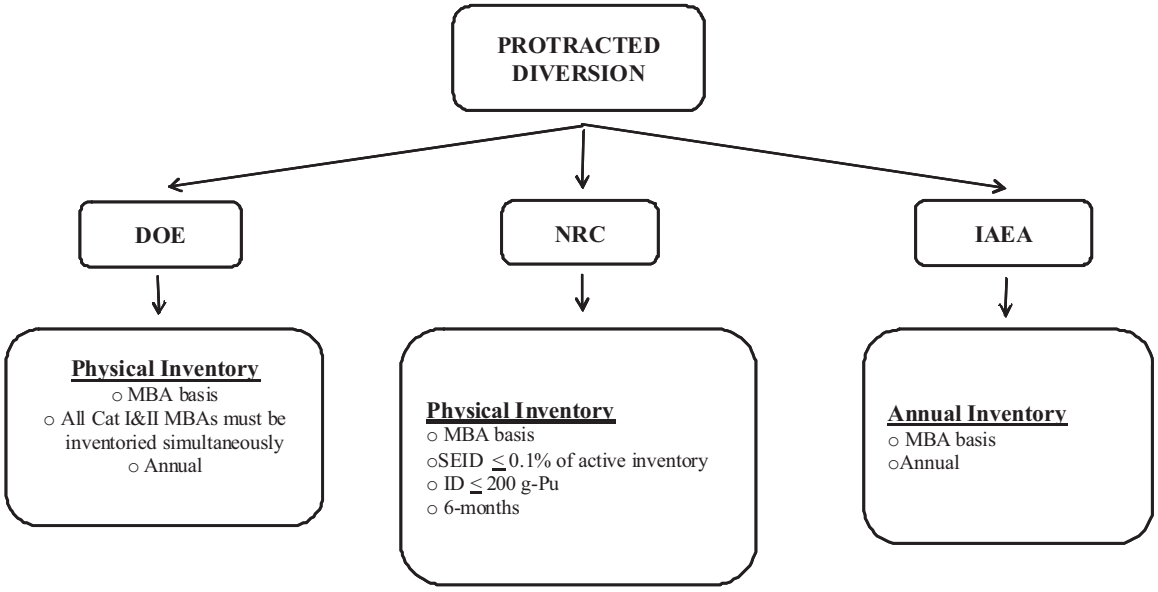


Figure D-3. Protracted diversion accountancy requirements for each regulating agency.

D-2.1 MC&A Inventory Requirements from the DOE Manual

Physical Inventories. The site/facility operator must implement a physical inventory program for nuclear materials to demonstrate that materials are present in their stated quantities and to detect the unauthorized removal of nuclear materials. Inventory requirements for separated Np-237 and separated americium are the same as for SNM. When facilities are precluded from performing physical inventories as required by this manual, material control and protection features must be enhanced to ensure inventory integrity. Physical inventory programs must comply with the following requirements.

Periodic Physical Inventories. Periodic and special physical inventories must be performed for each MBA according to the strategic importance of the material and the consequence of its loss.

1. Conduct of Physical Inventories. Inventories must be based on measured values, including measurements or technically justifiable estimates of holdup. Process monitoring techniques may be used for material that is undergoing processing and recovery operations and is inaccessible for measurements. Plans and procedures must be developed and documented that define responsibilities for performing inventories and specify criteria for conducting, verifying, and reconciling inventories. Statistical sampling, based on graded safeguards, may be used to verify the presence of items during inventories. Parameters for statistical sampling plans must be defined by the site/facility operator, and approved by the DOE-cognizant security authority. Sampling plans must specify the population, confidence level, minimum detectable defect, definition of a defect, and action to be taken if a defect is encountered.

   Table D-2, Minimum Sampling Parameters for Physical Inventories, provides minimum sampling parameter values for safeguards categories. The inventory population must be stratified according to item category as shown in Table D-2, taken from "Minimum Sampling Parameters for Physical Inventories", page II-3, Table II-1, Section A, DOE M 470.4-6 8-26-05 Inventories. Separate samples must be derived for each inventory stratum.

Table D-2. Minimum sampling parameters for Physical Inventories. (DOE M 470.4-6)

Category	Confidence level	Minimum Detectable Defect
I	95%	3%
II	95%	5%
III & IV	95%	10%

2. Physical Inventory Frequencies. Physical inventories must be performed for Category I and II MBAs that involve activities other than processing at a frequency determined by the DOE-cognizant security authority but at least semiannually (once every 6 months). The site/facility operator must ensure that physical inventories are performed bimonthly (once every 2 months) in Category I and II MBAs where processing occurs.

In processing areas where process controls provide equivalent levels of theft and diversion detection, physical inventories may be performed upon completion of the material campaign. In such cases, the DOE-cognizant security authority must approve a processing plan before starting the campaign. The process plan must identify compositions and quantities of material to be processed, projected processing timetable, process control measures used, and procedures necessary for material controls during process interruptions. Other factors to be considered for frequency determination include personnel radiation exposure, the operational mode of the facility, and credible protracted diversion scenarios.

At least annually, each facility must perform a simultaneous physical inventory of all Category I and II MBAs for which the established inventory frequency is annual or more frequent. MBAs with extended inventory frequencies of greater than 1 year are excluded from this requirement.

Physical inventories for Category III and IV SNM MBAs must be performed at a frequency specified by the DOE-cognizant security authority, but at least every 2 years (every 24 months). Category IV source and other nuclear material in Category I and II MBAs must be inventoried at least every 2 years (every 24 months), except when the source and/or other nuclear material is a credible substitution material.

When source or other nuclear materials are credible substitution materials for SNM and are collocated with SNM, facilities must inventory substitution materials with the same frequency as the SNM and use inventory measurement methods that can distinguish between SNM, source, and other nuclear material.

Except for materials required to be protected as SNM and potential substitution materials collocated with SNM, source and other materials outside Category I and II MBAs must be inventoried at a frequency approved by the DOE-cognizant security authority and as documented in the MC&A plan.
DOE M 470.4-6 Section A 8-26-05 II-5

In addition to the requirements listed above, inventory checks for Category IA items not in storage must be performed weekly for physical count verification and monthly for serial number verification. Inventory checks for stored Category IA items must consist of a physical count whenever the storage area is accessed and monthly serial number verification.

D-2.2 NRC – Inventory Requirements from 10 CFR 74

As interpreted for licensing of the Pu Disposition U.S. MOX Fuel Fabrication facility.

D-2.2.1 Abrupt Diversion

Process Monitoring is the terminology used by NRC to measure Abrupt Diversion. It shall be used to measure the inventory difference at least every three days for a Category IA Control Unit, and every seven days for a Category IB. A Control Unit may have fewer processing units than an MBA, but not necessarily. The measurement system for Abrupt Diversion must be capable of detecting 2 kg-Pu, which is equivalent to 5 formula-kg, with high confidence of detection. This is conducted during plant operation.

D-2.2.2 Protracted Diversion

A Physical Inventory is conducted at least every six months on an MBA basis, and includes process cleanout. The measurement performance must yield a Standard Error in the Inventory Difference less than or equal to 0.1% of active inventory. Active inventory is defined as process inventory at the beginning of the period plus cumulative throughout during the inventory period. The initial process inventory should be near zero for most MBAs, with the exception of vaults and buffer storage areas. The measured inventory difference must be less than or equal to 200 g-Pu. An inventory difference in excess of 200 g-Pu requires reporting to the NRC.

D-2.3 IAEA Recommendations

Implementation of International safeguards under the IAEA assumes physical inventories are conducted by the facility operator at frequencies, and with accuracies to close the material balance to meet established detection goals. Inventory preparation and inventory taking is the responsibility of the operator with the inventory listing provided to the IAEA through the national authority. The IAEA takes the responsibility to verify the reported inventory.

In making an inventory measurement, the facility operator wishes the accuracies of both the mass input and inventory measurements to be such that the error of the difference in the mean measurements will be less than 1 significant quantity of SNM at a stated confidence level. For plutonium, the significant quantity has been established as 8 kg and this implies that the measurement system must be capable of detecting 8 kg-Pu with high confidence. (The standard deviation, σ, or equivalently "The Limits of Error in the Inventory Difference"), represents the cumulative measurement uncertainty propagated over the measurements used in the material balance calculation. It is usually expressed at the 3-σ limit. The IAEA has defined high confidence as $3.3\ \sigma < 1$ significant quantity or for this case $\sigma < 2.4$ kg-Pu.

The IAEA has established the timeliness goal for detection of the plutonium goal quantity as 30 days for bulk processing facilities such as those at the back end of the fuel cycle. Operations of continuous processing large throughput bulk facilities preclude the possibility for frequent traditional shut down and flush-out inventories for material balance closure to meet the timeliness and goal quantities. The IAEA expects an annual shutdown and flush-out Physical Inventory Taking (PIT) and retains the responsibility for verification of this inventory, referred to as Physical Inventory Verification. However, the IAEA

typically expects the taking and reporting of an interim inventory on a 30-day basis to meet the timeliness goal. This is typically referred to as the Interim Inventory Taking (IIT) with the verification application referred to as the Interim Inventory Verification (IIV). The process of closing the material balances with the IIT and IIV is typically referred to as Near-Real-Time Accounting (NRTA). The challenge here is to perform the IIT, without shutdown and flush-out, whilst the facility is in normal operation.

As the IAEA has faced the challenge of implementing international safeguards in very large scale bulk processing facilities, they have recognized that with propagated uncertainties of the IITs and the throughput quantities over a 30-day period, the IIV process cannot meet the detection goals. In very recent cases, the IAEA has required similar IIT procedures at a higher frequency, on the order of 7–10 days with evaluation of multiple IITs over the 30-day period to achieve sensitivity at the goal quantity level. These frequent IITs are also subject to verification and have been designated as Special Inventory Verifications.

As noted, the IAEA does not conduct inventories, only verifies the reported data. In order to structure the verification process, the IAEA stratifies the reported inventories by quantities and then applies statistical methods to select the number of reported inventory values (samples) to be selected for verification.

D-3. EXAMPLE OF APPLICATION OF MATERIAL CATEGORY REQUIREMENTS (AFCF)

The DOE GNEP strategy envisages the construction of a nuclear facility in the U.S. for industrially representative demonstration of the major fuel recycling stages including thermal and fast reactor reprocessing, lead test fuel assembly fabrication and waste partitioning and immobilization. This advanced demonstrator is known as the Advanced Fuel Cycle Facility (AFCF). Conceptual design is of AFCF is underway and has included safeguards and security design including efforts described in this section (GNEP, 30% Conceptual Design Report for AFCF), DOE NE, January 26, 2007). Table D-3 shows the DOE graded safeguards values and gives the present material category definitions now under review.

Table D-3. DOE graded safeguards table (DOE M 470.4-6 Chg 1, Section A, Page I-10, Table I-4).

	Attractiveness Level	Pu/U-233 Category (kg)				Contained U-235/Separated Np-237/Separated Am-241 and -243 Category (kg)				All E Materials Category IV
		I	II	III	IV[1]	I	II	III	IV[1]	
WEAPONS Assembled weapons and test devices	A	All	N/A	N/A	N/A	All	N/A	N/A	N/A	N/A
PURE PRODUCTS Pits, major components, button ingots, recastable metal, directly convertible materials	B	≥2	≥0.4<2	≥0.2<0.4	<0.2	≥5	≥1<5	≥0.4<1	<0.4	N/A
HIGH-GRADE MATERIALS Carbides, oxides, nitrates, solutions (≥25 g/L) etc.; fuel elements and assemblies; alloys and mixtures; UF_4 or UF_6 (≥ 50% enriched)	C	≥6	≥2<6	≥0.4<2	<0.4	≥20	≥6<20	≥2<6	<2	N/A
LOW-GRADE MATERIALS Solutions (1 to 25 g/L), process residues requiring extensive reprocessing; moderately irradiated material; Pu-238 (except waste); UF_4 or UF_6 (≥ 20% < 50% enriched)	D	N/A	≥16	≥3<16	<3	N/A	≥50	≥8<50	<8	N/A
ALL OTHER MATERIALS Highly irradiated forms, solutions (<1 g/L), uranium containing <20% U-235 or <10% U-233[2] (any form, any quantity)	E	N/A	N/A	N/A	Reportable Quantities	N/A	N/A	N/A	Reportable Quantities	Reportable Quantities

[1]The lower limit for Category IV is equal to reportable quantities in this Manual.
[2]The total quantity of U-233 = [Contained U-233 + Contained U-235]. The category is determined by using the Pu/U-233 side of this table.

D-3.1 AFCF Category – Head End

Consistent with earlier flow-sheets, this area starts with whole irradiated fuel assemblies and ends with filtered dissolver solution. It also includes undissolved solids treatment. It is conceivable, under the distributed existing facilities concept, that this could be broken into a spent fuel chopping area, and a spent fuel dissolution area. Undissolved solids treatment could also be separated out, but the initial filtering of undissolved solids would probably occur in the dissolving area.

All of these materials are “highly radioactive,” probably including aged spent fuel. So, these materials would all be attractiveness level “E” and the Category of the area would be IV, no matter the quantity of material handled.

D-3.2 AFCF Category – Aqueous Separations

This area starts with clarified dissolver solution and ends with a dilute TRU solution and various waste streams. It is conceivable that the UREX+ chemical separations process could be broken down into sections that are distributed across several areas. It is also conceivable that one area would be used but only one part of the UREX+ process would be run at one time (that is, run all of one separation step before proceeding to the next step).

The solutions become progressively less radioactive in the downstream separation steps. However, Pu (and other actinide) concentrations are always below about 4 g/l. Attractiveness would range from “E” to “D,” making the Category IV to II. To achieve Category II, the area would have to contain at least 16 kg of Pu in materials that are not “highly radioactive” (at least 4,000 liters of stored TRU solution). (Note that attractiveness level descriptions are expected to be changed soon by DOE. It is anticipated that attractiveness level “E” will be more difficult to apply; that is, some materials currently considered “E” would likely become classified as “D” or even “C.”)

D-3.3 AFCF Category – Product Solidification

In AFCF, this encompassed the TRU solidification, as well as the waste/byproduct steams. The liquids would be reduced in volume and then solidified by a means specific to the final form. In a distributed scenario, each stream could be processed in a different area, or one area could be used on a campaign basis to process one material at a time. As envisioned in AFCF, U would not be blended back into TRU until fuel fabrication.

Attractiveness of the waste streams would be expected to be "E" or "D," depending upon the radiation level (note – the cutoff level may be changing) and SNM concentration. It is possible that the TRU content of waste streams could be low enough to make these streams of no significance for accounting. Category, if these contain SNM, would be IV to II. Category II would be achieved if "D" material is present at a mass greater than 16 kg.

Attractiveness of the TRU stream would change from "D" for the dilute solution to "C" for solid, oxide product (it is anticipated that the TRU product will not be "hot" enough to qualify for "D" or "E" attractiveness; in addition, as the TRU stream is further partitioned, as in many UREX+ flow-sheets, the radiation level of the Pu/Np would be decreased, further warranting attractiveness "C."). Category could be as high as I for the TRU product; this is achieved at attractiveness "C" with at least 6 kg of Pu.

D-3.4 AFCF Category – Fuel Fabrication

Oxides being the example, this area would take solidified TRU product and blend in U to the U/TRU composition desired for the lead test assemblies. Once the final blend is achieved, pellets are made, and rods and assemblies are manufactured. In a distributed scenario, these activities could be distributed over several areas – blending, pellet production, rod production, assembly and fuel production. Blending probably requires its own unique area (aqueous processing), but the other activities could be campaigned through one area.

The starting attractiveness (TRU oxide product) is expected to be "C." The attractiveness could be reduced to "D" with the addition of sufficient U. Over 6 kg of "C" Pu will make the area Category I. The attractiveness of the rods and assemblies is expected to be the same as the pellets. Under DOE rules, it may be possible to argue that the assemblies are too large and heavy to be of concern to achieve an exception for a lower attractiveness level.

D-3.5 AFCF Category – Electrochemical Process

Starting material is spent fuel; product is a U/TRU metallic ingot. In AFCF, metal fuel fabrication would have occurred in a different area. All of the electrochemical processing would be expected to occur in the same area, even in a distributed scenario.

Very little is known about the final composition (impurities) of the U/TRU product; this discussion is based upon sufficiently "clean" material that radiation is not a factor in determining attractiveness. So, it is likely that the product material would be attractiveness "B" or "C," depending upon the U/TRU ratio. An argument can be made to treat this material as "B" only when it is removed from the electrochemical processing area, since that area would be expected to be highly radioactive. At attractiveness "B" it takes just 2 kg Pu to reach Category I.

D-4. EXAMPLE OF INTERNATIONAL SAFEGUARDS FOR PLUTONIUM BULK HANDLING FACILITIES – ROKKASHO-MURA REPROCESSING PLANT

The most significant and extensive effort of international safeguards implementation was associated with the Japanese Rokkasho-mura Reprocessing Plant (RRP), and this is most representative of IAEA points of interaction under Safeguards-by-Design for future large-scale Pu bulk handling facilities. Large scale Pu processing facilities, such as the RRP, pose significant challenges to the IAEA. The Design Information Questionnaire (DIQ) for the RRP was submitted in the late 1980s. The prospect of safeguards for the RRP was so challenging to the IAEA that a special forum of nations with the reprocessing technology was convened. This was referred as the LASCAR (Large Scale Reprocessing) Exercise (IAEA -Johnson et al 1992). It resulted in recommendations for safeguards implementation at such facilities and influenced the period of negotiation of the Facility Attachment.

The DIQ, while requiring general information on the facility, location, ownership and general process information, also requires an initial description of measurements and measurement points. Implementation of International Safeguards under the IAEA assumes physical inventories are conducted by the facility operator at regular intervals, and with measurement accuracies for inventory and flow measurements to close the material balance to meet established detection goals. Measurement of flows, inventory preparation and inventory taking is the responsibility of the operator with the inventory listing provided to the IAEA through the national authority. The IAEA verifies the inventory of nuclear material declared by the facility operator in accordance with the IAEA safeguards criteria in the Safeguards Manual, the Safeguards Approach, and the Facility Attachment.

The operator must demonstrate overall measurement uncertainty, including the physical inventories involved, at less than one significant quantity of SNM with "high confidence." For plutonium, the significant quantity is established as 8 kg. High confidence has traditionally been established at the 95% confidence level or roughly 2 times the standard deviation of the uncertainty of the material balance. These requirements are described in greater detail in Appendix D.

The IAEA timeliness goal for the detection of a diversion of un-irradiated plutonium is thirty days. (For clarification, this is irrespective of whether the un-irradiated plutonium is reactor-grade, weapons-grade, mixed with uranium in the form of MOX, or at facilities other than reprocessing plants. It is established based on the material type, un-irradiated plutonium.) Operation of continuous process, large throughput bulk facilities precludes the possibility for inventory measurement using traditional shut down and flush-out for material balance closure to meet the timeliness and goal quantities. The IAEA expects an annual shutdown and flush-out with physical inventory taking (PIT) on an annual basis and retains the responsibility for verification of this inventory, referred to as Physical Inventory Verification. To meet the timeliness goal in facilities that process un-irradiated plutonium, the IAEA conducts interim inventory determinations at least every thirty days. This is typically referred to as the Interim Inventory Taking (IIT) with the verification application referred to as the Interim Inventory Verification (IIV). The process of closing the material balances with the IIT and IIV is typically referred to as Near-Real-Time Accounting (NRTA). The challenge here is to make the IIT with the facility in normal operation.

In practice, the facility operator takes the annual physical inventory and the IAEA verifies the inventory. However, the IIV is an inspection activity that does not coincide with the ending of a material balance period and does not necessarily have to include all nuclear material present in the material balance area (MBA). Under the typical safeguards agreement, verification is made possible for purposes of timely detection (of diversion) or for re-establishment of the inventory of nuclear material, within an area covered by containment/surveillance, or after a failure of surveillance (IAEA Safeguards Glossary – 2001 Edition, "Interim Inventory Verification (IIV)," paragraph 6.53). The relevant point is that the IAEA does take inventory, as well as verifies the inventory, during an IIV. It is true that the facility operator

takes this inventory as well, in advance of the IAEA, in order make their declaration of nuclear material in the area. But the IAEA independently takes and verifies this inventory. This is done using IAEA controlled installed and portable instruments, and in some cases using the operator's instruments. If the operator's instruments are used, suitable measures will be taken to authenticate the results and ensure that the safeguards conclusions drawn by the IAEA are independent of the facility operator or national authorities (IAEA SGTS/TIE Policy Paper #20, "Joint Use of Safeguards Equipment, April 20, 2006).

As the IAEA has faced the challenge of implementing international safeguards in very large scale bulk processing facilities, they have recognized that with propagated uncertainties of the IITs and the throughput quantities over a 30-day period, the IIV process cannot meet the detection goals. As the Facility Attachment negotiations for the RRP progressed, the IAEA has required similar IIT procedures at a higher frequency, on the order of 7–10 days with evaluation of multiple IITs over the 30-day period to achieve sensitivity at the goal quantity level. These frequent IITs are also subject to verification and have been designated as Short-term Inventory Verifications.

During the verification process, the IAEA stratifies the nuclear material by element and material type. In a reprocessing plant, examples would be plutonium in spent fuel, dissolver solution, process solution, waste and MOX product. The IAEA uses a random sampling plan and algorithm in accordance with the IAEA Safeguards Criteria and Manual to detect diversions of nuclear material. This is done with variable accuracy to detect bias, partial and gross defects.[a] If statistically significant differences between the operator's declaration and the inspector's verified results are observed, the inspectors will increase the number of samples and use more accurate methods to determine if there are actual discrepancies or anomalies in the operator's declaration. It is important to remember that it is the responsibility of the facility operator to make all safeguards-related measurements and report them through the national authority to the IAEA. It is the responsibility of the IAEA to verify the declarations, using independent measures as much as possible. The LASCAR exercise strongly recommends the use of operator instruments for verification, as much as possible. But recent concerns raised within the IAEA have tended to move away from the use of operator instruments back to independent measures.

The LASCAR exercise recognized international safeguards will likely need additional measures beyond traditional material balance and even NRTA to meet the detection goals. Process monitoring, coupled to additional surveillance systems, would also be required. The details of these additional measures are also a part of the extended negotiations of the facility attachment.

In the case of the RRP, the DIQ was submitted during the late 1980s. The facility construction and initial commissioning activities were completed in early 2006 and the Safeguards Approach was completed and agreed. Mapping the negotiation of the Facility Attachment to the Safeguards-by-Design process, with the CD phases as defined by DOE procedures, requires several key phases of the process to be completed along the timeline. The LASCAR exercise was definitive concerning decisions on instrumentation requirements and placements being made as early as possible in the design. Designing installations for safeguards assay equipment in advance is preferred to retrofitting facilities by cutting penetrations in walls or adding utility services, where they were not provided in the original design. It is inefficient and uneconomic, although still possible, to make these changes to accommodate safeguards equipment if the facility has not yet started up. However, retrofitting the facility in the process areas can be nearly impossible after start-up, if the facility handles highly radioactive material or plutonium.

Then there is the installation of equipment. The nature of international safeguards requires IAEA to maintain control of their instrumentation. IAEA-owned equipment must be installed in secure IAEA-owned apparatus and installation of that equipment, by independent contractors under contract to the

a. Bias defects are on the level of uncertainty using destructive analysis. Partial defects refer to missing a portion or part of the nuclear material – e.g., removal of fuel pins from a spent fuel assembly. Gross defects refer to the gross attributes of the nuclear material – i.e., is the plutonium present or not, e.g., does the material have a radiation attribute characteristic of plutonium in spent fuel, or not.

IAEA, must be phased with plant construction. There is the lead time for design and procurement of IAEA equipment, as well as the scheduling phase to organize the installation. This is another important part of the Facility Attachment negotiation period.

In the event that on-site laboratory facilities are required, this is another major design decision that must be complete before construction starts. Equipment procurement and installation again must be coordinated. It is not a trivial matter to obtain IAEA design criteria and incorporate those into the facility design. Needs subsequent to start-up and into operations must be addressed early, since there are utility supply considerations. There is usually a negotiation between the facility operator and the IAEA for handling of radioactive wastes, etc. Facilities to accommodate inspectors, computer systems and file storage requirements must be negotiated before construction to assure proper space is allocated within the constraints of access control and security.

The DIV process also has an influence throughout the period of Facility Attachment. As the facility is built, the IAEA negotiates when and what equipment is subject to DIV. In the case of the RRP, there was a close dialog through the construction period to provide schedules for equipment installation and calibration activities, for instance, to ensure the IAEA could schedule inspectors for selected activities. For example, with the proper coordination, the IAEA could inspect parts of the plant that are intended to be closed off after completion. With properly designed sealing hardware on the access points and correct timing, IAEA inspectors could both inspect and seal a location as part of their DIV activities, saving both the Operator and the IAEA time. Part of the DIV process is to provide the inspectors with actual facility construction documents to allow verification. These documents, in many cases, represent proprietary information that must be controlled. In the case of RRP, these documents were stored in sealed cabinets with dual control by the IAEA and the national authority.

The commissioning phase is a period when components and then systems are systematically accepted after construction. This is another phase that must be coordinated with the IAEA to ensure they have the opportunity to accept their systems during the scheduled phases. A complex facility, such as a bulk processing fuel cycle facility, will likely require an extensive data collection and evaluation system for the IAEA. Development, installation, and functional testing during commissioning must also be coordinated. As the Facility Attachment is finalized just prior to final commissioning, the IAEA takes the elements of the Facility Attachment to prepare the Safeguards Approach document. This document will specifically define all authorized inspection activities, equipment to be used, and the inspection procedures. This document must be in place by commencement of operations as the basis of what will be done by IAEA inspectors.

Although the IAEA verifies the design of the facility during construction and start-up, it continues to periodically re-verify the facility design during plant operation up until the point of decommissioning. Unlike the construction phase, these activities are less frequent, but are still performed at least annually. This is done in order to detect safeguards-relevant changes in the plant, such as an increase in plant capacity, installation of undeclared process equipment, or installation of undeclared removal pathways for nuclear material. The specific procedures to accomplish this activity along with required equipment and procedures must also be defined during the period of negotiation of the facility attachment. The best practice case of IAEA safeguards for RRP, which did not include SBD (see Appendix H-2), shows that further improvements are still possible.

Appendix E

Flowcharts of Safeguards-by-Design Process for DOE Domestic Regulatory Environment

Appendix E
Flowcharts of Safeguards-by-Design Process for DOE Domestic Regulatory Environment

E-1. SBD FLOWCHARTS FOR DOE DESIGN AND CONSTRUCTION

The SBD process is a systematic and structured series of steps directed to fully integrating international and national safeguards, physical security, and other proliferation barriers into the design and construction process for nuclear facilities, with the objective of increasing the safeguardability, protectability, and proliferation resistance of facilities. As explained in Volume 1, Section 3.1, the optioneering study generated a single process covering domestic and international (IAEA) safeguards. However, the study was performed in two stages: first, a process was developed using DOE domestic requirements and SBD team's performance requirements only (see Section 3.2), and second, the first results were modified to integrate the additional effects of incorporating international (IAEA) requirements (see Section 3.3). The step-wise approach was to simplify the study and facilitate its visual representation by means of two series of flowcharts, the present appendix (domestic environment) and Appendix G (domestic environment and international safeguards).

Each of the following flowcharts outlines the SBD process in the DOE facility acquisition process; each design phase ends with the successful completion of a critical decision point. The DOE critical decision points are process checkpoints that specify that specific requirements that are needed to be met and approved to continue with subsequent steps in the design process. The flowcharts show three distinct levels that demonstrate the interactions between domestic safeguards activities (initiated by the Safeguards-by-Design Team [SBDT])), Project Engineering, and Program and Project Management. The Program and Project Management group operates as project leadership. The Project Engineering group uses the guidance provided by the Program and Project Management group and further manages the project by interacting with the SBDT. The following the flowcharts diagrams, there are descriptions of SBD process requirements. A fuller textual discussion of the SBD process is given in Volume 1, Section 3. The SBD process uses the basic process flow charts originated for Safety-in-Design as provided in DOE STD-1189-2008, March 2008, Integration of Safety into the Design Process.

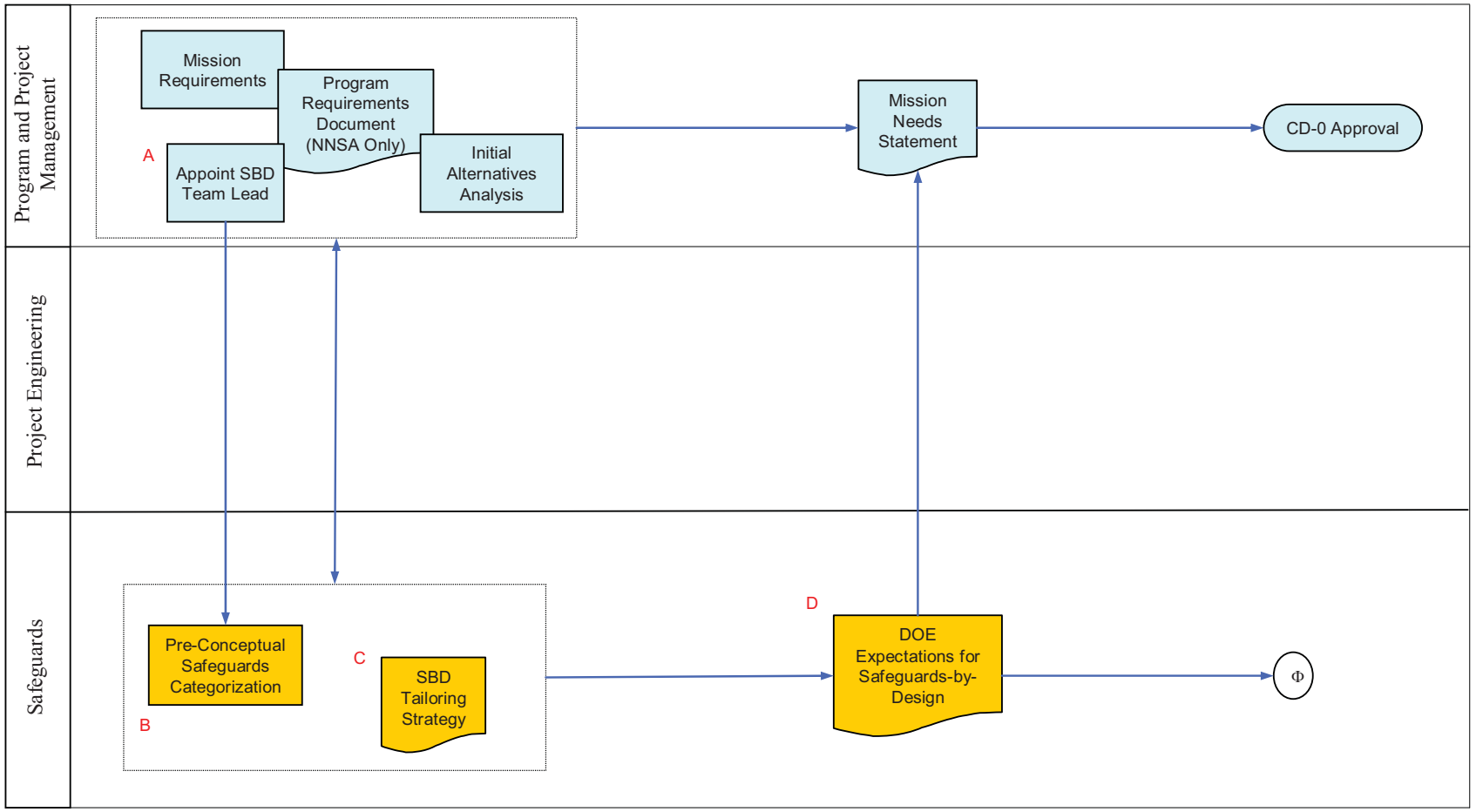


Figure E-1. Safeguards-by-Design Process (DOE) – Initiation Phase.

Letter	Description
A.	**Appoint Safeguards-by-Design Team Lead** – The individual designated to lead the SBD team, is appointed early in the pre-conceptual planning to lead the efforts to characterize the facility targets and vulnerabilities and categorize the facility from a safeguards perspective. This individual is responsible for preparing the Safeguards-by-Design tailoring strategy.
B.	**Pre-Conceptual Safeguards Categorization** – DOE safeguards and security programs are established through the DOE 470 series Orders and Manuals. DOE assets are defined and protection standards outlined in DOE O 470.3A, *Design Basis Threat Policy* (U). Depending on the asset being protected, protection strategies range from a combination of compliance with DOE security policies to specific performance standards that should be met. For those design assets designated as Threat Level 1, 2, or 3, the design basis threat policy should be referenced because additional performance-based security measures may necessitate a vulnerability assessment to be performed to determine what additional security measures are necessary to achieve an integrated protection system. The DOE O 470 series of directives establishes minimum design principles. DOE defines reportable elements and their isotopes. Nuclear materials are controlled and accounted for on the basis of categorization according to strategic or financial importance and potential environmental threat. Attractiveness levels and safeguards categories are defined.
C.	**Safeguards-by-Design Tailoring Strategy** – The Safeguards-by-Design Tailoring Strategy documents the project's consideration of the Safeguards-by-Design principles, key concepts, and approach in the governing standard. It describes, at a summary level, the way that the project proposes to implement these principles in the project, including any exceptions or alternative approaches judged more appropriate for the project. This document identifies the major safeguards and nonproliferation documentation deliverables and the associated governing requirements to be provided within each project phase. The tailoring strategy is incorporated into the Safeguards Design Strategy document developed during conceptual design.
D.	**DOE Expectations for Safeguards-by-Design** – The DOE Expectations for Safeguards-by-Design describes the requirements and approach that DOE expects the project to employ in integrating safeguards into the project commensurate with the information available about targets, potential vulnerabilities, and candidate safeguards measures. This document also documents the DOE review of the tailored application of Safeguards-by-Design principles, key concepts, and approaches proposed in the tailoring strategy. This review also considers areas, such as design basis threat, where additional safeguards margin is appropriate given the design life of the facility. This document is a key input to the Safeguards Design Strategy document prepared by the project in the conceptual design phase.
E.	**Create Safeguards-by-Design Teams** – The project manager establishes the Safeguards-by-Design Team to support the project team in ensuring the integration of safeguards, security, and proliferation barriers into the design process and to manage the preparation of safeguards and security deliverables required to support each critical decision.
F.	**Safeguards Design Strategy** – The Safeguards Design Strategy is a tool to guide project design, SG design documentation development planning, and it provides approving authorities sufficient information upon which to base decisions. It provides a single, integrated source for the SG design policies, philosophies, major requirements, and goals for the project. The SG Design Strategy includes a section that identifies the major targets and threats anticipated in the facility and how those targets will be protected. Any risks to these decisions from evolving threats should be identified. In addition, the SG Design Strategy identifies major safeguards documentation deliverables to be provided within each project phase. The SG Design Strategy is expected to be revised and updated as the project matures.

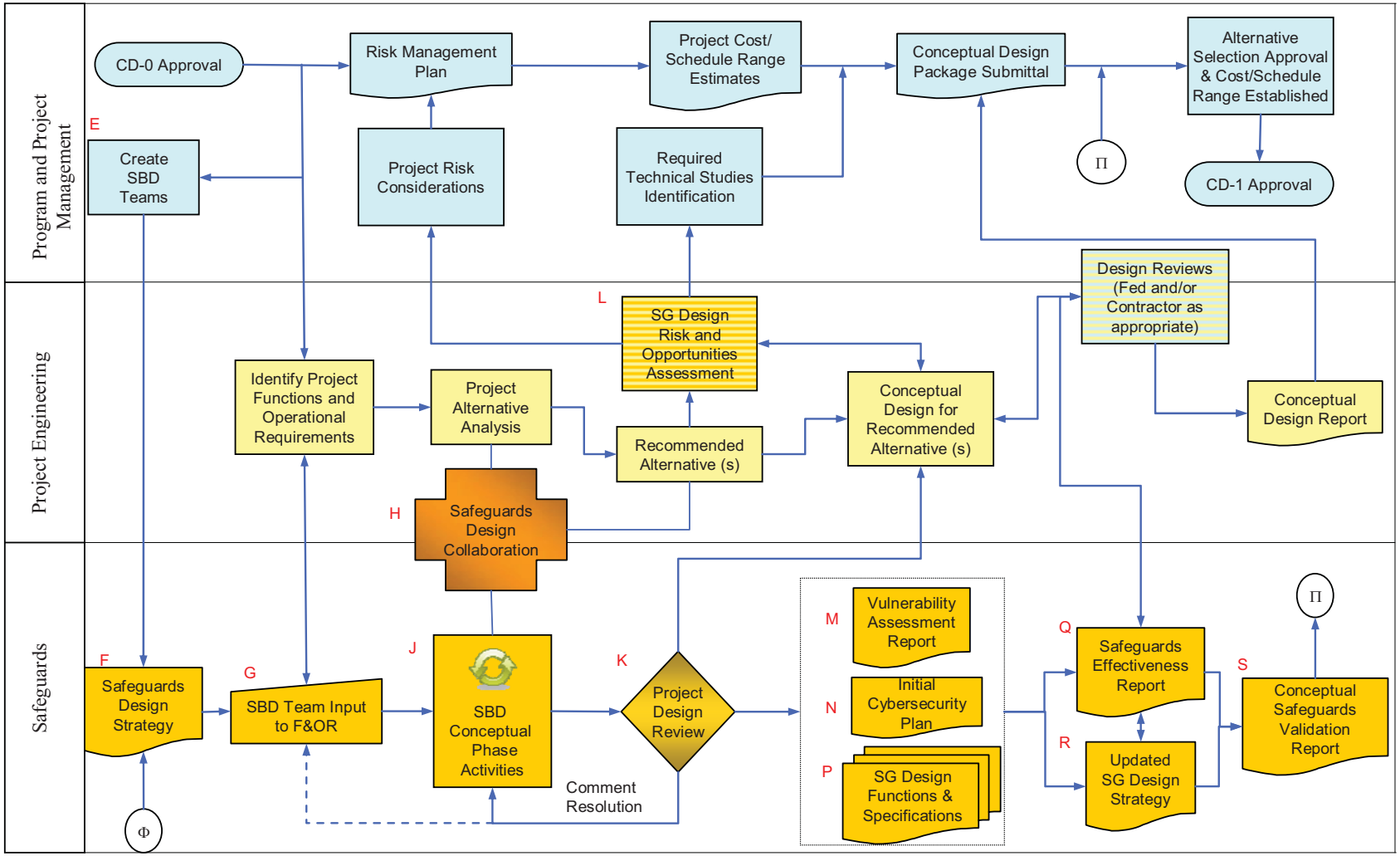


Figure E-2. Safeguards-by-Design process (DOE) – Definition Phase.

Letter	Description
G.	**Safeguards-by-Design Team Input to F&OR** – For a successful project and following Mission Need approval (CD-0), a complete and clear statement of functional and operational requirements (F&OR) must be generated and analyzed for iterative discussion with and approval by stake-holders. Completely analogous to other disciplines, including safety-in-design, the SBD team identifies those high-level requirements that must be fulfilled in order to achieve the desired safeguards performance. The relevant requirements may be a combination of existing regulations, where available, and additional items to meet anticipated future regulatory developments or individual facility/site needs. Note that F&OR often state necessary capabilities and constraints, but normally do not prescribe in detail 'how' those needs are to be met.
H.	**Safeguards Design Collaborations** – The SBD team utilizes early information exchange through scheduled meetings and informal communications with the other project design teams, especially safety. Early, frequent, and open communications among design team members are crucial to the overall project success.
I.	For clarity, this letter is not used.
J.	**Safeguards-by-Design Conceptual Phase Activities** – The Safeguards-by-Design Conceptual Phase activities are described by the "SBD Design Loop." As the design progresses, changes and updates will be shared with the SBD Team. The SBD team will then cycle through their analyses. The threats and issues definitions will be reviewed and updated as necessary. The identified assets, targets, and risks will be reviewed and updated, then ranked. Facility and system designs or updates to mitigate the risks are developed. The outcome is analyzed (VA, exercises, etc.) and assessed versus the requirements and criteria. The SBD team then optimizes over the design, requirements, and criteria. This loop is performed as necessary until the SBD team is satisfied with the outcome, and then the design cycle passes back to the overall project team for project design review.
K.	**Project Design Review** – A review of the safeguards design, by an external (to the SBD Team) peer and project group, with a project-wide perspective.
L.	**Safeguards Design Risk and Opportunities Assessment** – The Safeguards Design Risk and Opportunity Assessment for the conceptual design is used to evaluate the overall project cost and schedule risks and opportunities associated with meeting the safeguards performance requirements. The risks include the uncertainties related to the possibility that there may be additional costs and schedule impacts that are not yet identified because the design is still immature or there are uncertainties associated with the safeguards viability of the design and programmatic strategies selected. Opportunities refer to the potential opportunities to reduce the costs or improve the schedules as the design matures and to select proposed safeguards measures or approaches or other cost and schedule drivers that are identified as not being necessary after all.
M.	**Vulnerability Assessment Report** – Vulnerability Assessment Report: DOE G 413.3-3 requires that a Vulnerability Assessment (VA) must be performed at the completion of each design phase. The process of conducting a VA is currently prescribed in DOE M 470.4-1. Performance testing must be conducted and the results included in the vulnerability assessment report (VAR) to calculate overall system effectiveness. The VAR is the end product and documents the results of a VA. The VARs must include targets analyzed, methodology used, system effectiveness results, parameters and assumptions under which the VA was conducted, and reference to evidence files.

Letter	Description

N. **Initial Cybersecurity Plan** – A security plan showing how the facility cyber resources will be protected from outside threats. This will include starting the SP 800-53 documentation to request Certification and Accreditation of the facility cyber resources. This plan will be updated as necessary in all phases of the design process. The cybersecurity plan is already and DOE requirement, and is considered within the SBD process because of the increasing use of IT throughout nuclear facilities for safeguards and security purposes. For projects including international safeguards, there is a special cybersecurity requirement to accommodate IAEA IT systems and instrumentation while providing secure communications.

O. For clarity, this letter is not used.

P. **Safeguards Design Functions and Specifications** – Early identification of the safeguard measures and systems relied upon to meet safeguard performance requirements (particularly those that could have high cost or schedule impacts) is a major contributor to developing an accurate estimate of facility and project costs. The vulnerability assessment establishes the foundation for identifying the physical protection measures and systems and their performance requirements. The MC&A process analysis, not currently specifically required by DOE directives, establishes the foundation for identifying nuclear MC&A measures and systems and their performance requirements. The proliferation barrier analysis, not currently required by DOE directives, establishes the foundation for identifying required proliferation barriers and their performance requirements. Identifying these Safeguards-by-Design functions and classifications (the measures and systems that comprise the physical protection, accountability, and proliferation design envelope) is a fundamental part of the safeguards-by-design process.

   a. **MC&A Process Analysis.** This 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. The analysis should be tailored to the complexity of the facility and the safeguards significance of the nuclear material housed at the facility. The MC&A process analysis should include an evaluation of the process sufficient, by the completion of final design, to support the development of the facility MC&A plan. The MC&A analysis may also include vulnerability assessment components, such as diversion path analysis.

   b. **Proliferation Barrier Analysis**. This analysis identifies the design features and associated system performance requirements needed to meet intrinsic and extrinsic proliferation resistance requirements, not yet fully defined, commensurate with the maturity of the design.

Q. **Safeguards Effectiveness Report** – A Safeguards Effectiveness Report (SER) is prepared and submitted to DOE during each principal design stage, i.e., conceptual, preliminary, and final design. The Safeguards Effectiveness Reports should be structured so that they may evolve into the facility MC&A plan and the facility-specific updates to the Site Safeguards and Security Plan (SSSP) as the design progresses through construction. Then the Final Safeguards Effectiveness Report can be directly used to produce these documents. Further updated versions may also be required prior to and during facility operations. For example, during conceptual design, the SER comprises:

   a. Requirements analysis

   b. Identification of key project interfaces affecting design decisions

Letter		Description
	c.	Analysis of SG design concepts and justification of preferred alternative
	d.	Safeguards Design Strategy (SGDS)
	e.	Vulnerability Assessment, which links to results of the PHA, DBT analysis, major facility safety functions and major SSCs
	f.	Initial SG Design Risk and Opportunities Assessment
	g.	Conceptual Safeguards Design (CSGD) which references the final conceptual design architecture given in the CDR, the conceptual Safeguards Design Strategy (SGDS), and baseline cost estimates
	h.	Identification of required technical studies to resolve risks and opportunities
	i.	DOE reviews the conceptual Safeguards Effectiveness Report (SER) and, if appropriate, prepares a Conceptual Safeguards Validation Report (CSVR). It is recommended to use safeguards design and assessment methodology that identifies performance vulnerabilities and can guide the use of resources to mitigate them.
R.		**Updated Safeguards Design Strategy** – Updated SG Design Strategy: Make any adjustments to the prepared project plan's policy and procedures on the management and control of the design process which may have been discovered lacking by the SBD design team.
S.		**Conceptual Safeguards Validation Report** – Produced by DOE after review of the Safeguards Effectiveness Report. It documents the review, resolution of comments, and their acceptance by DOE.

Note: Greek lettered connector symbols refer to connections between flowcharts in Appendixes E and G.

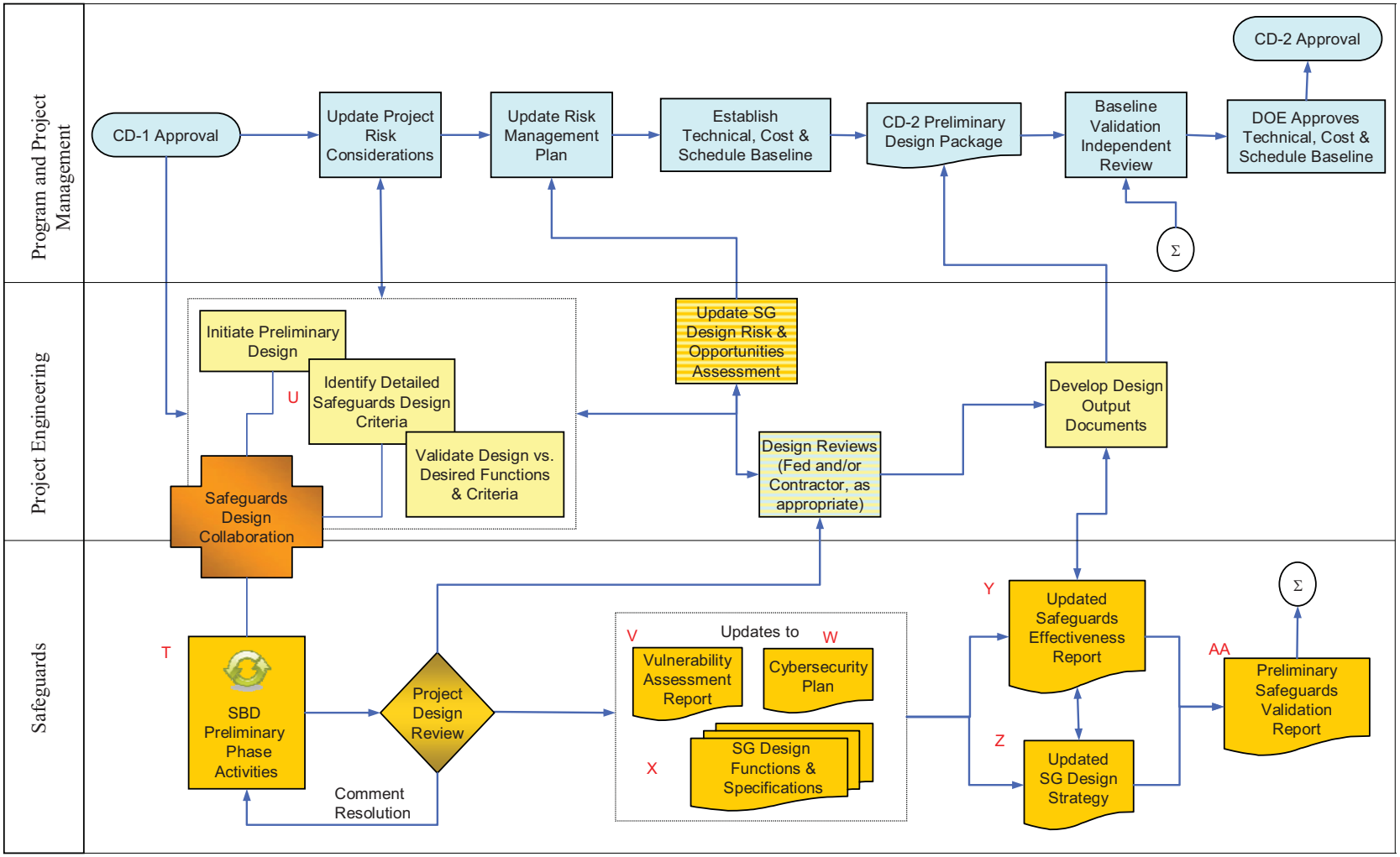


Figure E-3. Safeguards-by-Design process (DOE) - Execution Phase, Preliminary Design.

Letter	Description
T.	**Safeguards Preliminary Phase Activities** – As described in "J," with increased detail suitable for the preliminary design.
U.	**Identify Detailed Safeguards Design Criteria** – Clear and detailed documentation of the safeguards design criteria that follow from the F&OR.
V.	**Updates to Vulnerability Assessment Report** – Vulnerability Assessment Report, as described in "M." The level of detail and the particular analyses performed will be appropriate for the design progress to this point.
W.	**Updates to Cybersecurity Plan** – Cybersecurity Plan, as described in "N," updated for the current level of design progress.
X.	**Updates to Safeguards Design Functions and Specifications** – SG Design Functions and Specifications, as described in "P," updated with preliminary design details.
Y.	**Updated Safeguards Effectiveness Report** – Safeguards Effectiveness Report, as described in "Q," updated to reflect the more detailed status of the safeguards design.
Z.	**Updated Safeguards Design Strategy** – Update of the SGD strategy, as described in "F." This includes increased detail as appropriate for the preliminary design.
AA.	**Preliminary Safeguards Validation Report** – Update of the Safeguards Validation Report to document review and acceptance of the updated safeguards design.

Note: Greek lettered connector symbols refer to connections between flowcharts in Appendixes E and G.

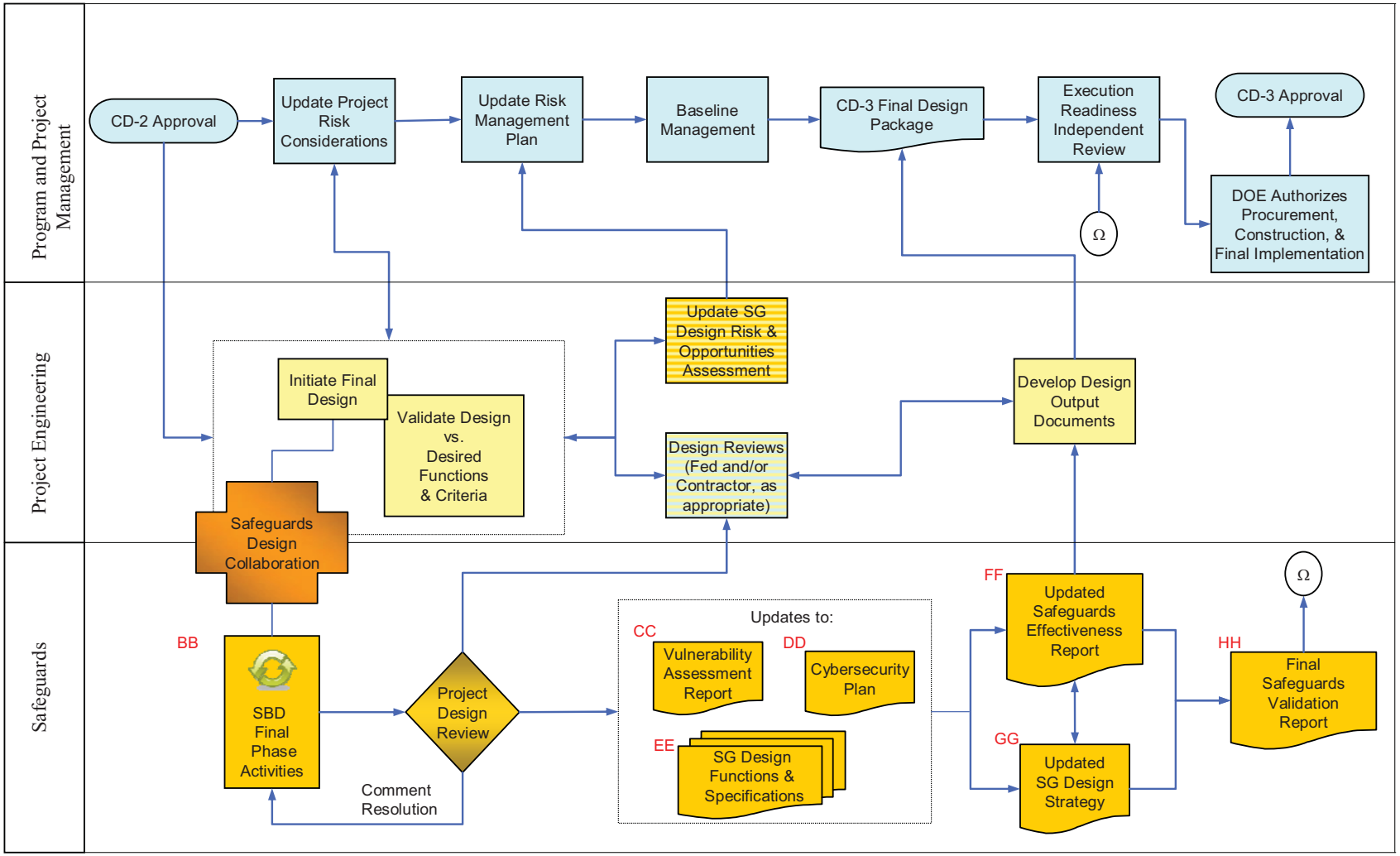


Figure E-4. Safeguards-by-Design Process (DOE) - Execution Phase, Final Design.

Letter	Description
BB.	**Safeguards-by-Design Final Phase Activities** – As described in "J," with increased detail suitable for the final design.
CC.	**Updates to Vulnerability Assessment Report** – Vulnerability Assessment Report, as described in "M." The level of detail and the particular analyses performed will be appropriate for the design progress to this point.
DD.	**Updates to Cybersecurity Plan** – Cybersecurity Plan, as described in "N," updated for the current level of design progress.
EE.	**Updates to Safeguards Design Functions and Specifications** – Update of the SG Design Functions and Specifications, as described in "P."
FF.	**Updated Safeguards Effectiveness Report** – Safeguards Effectiveness Report, as described in "Q," updated to reflect the more detailed status of the safeguards design.
GG.	**Updated Safeguards Design Strategy** – Safeguards Design Strategy, as described in "F," updated to reflect final design status and to include safeguards activities that will be performed during the construction and start-up phases.
HH.	**Final Safeguards Design Validation Report** – Update of the Safeguards Design Validation Report to document review and acceptance of the final safeguards design.

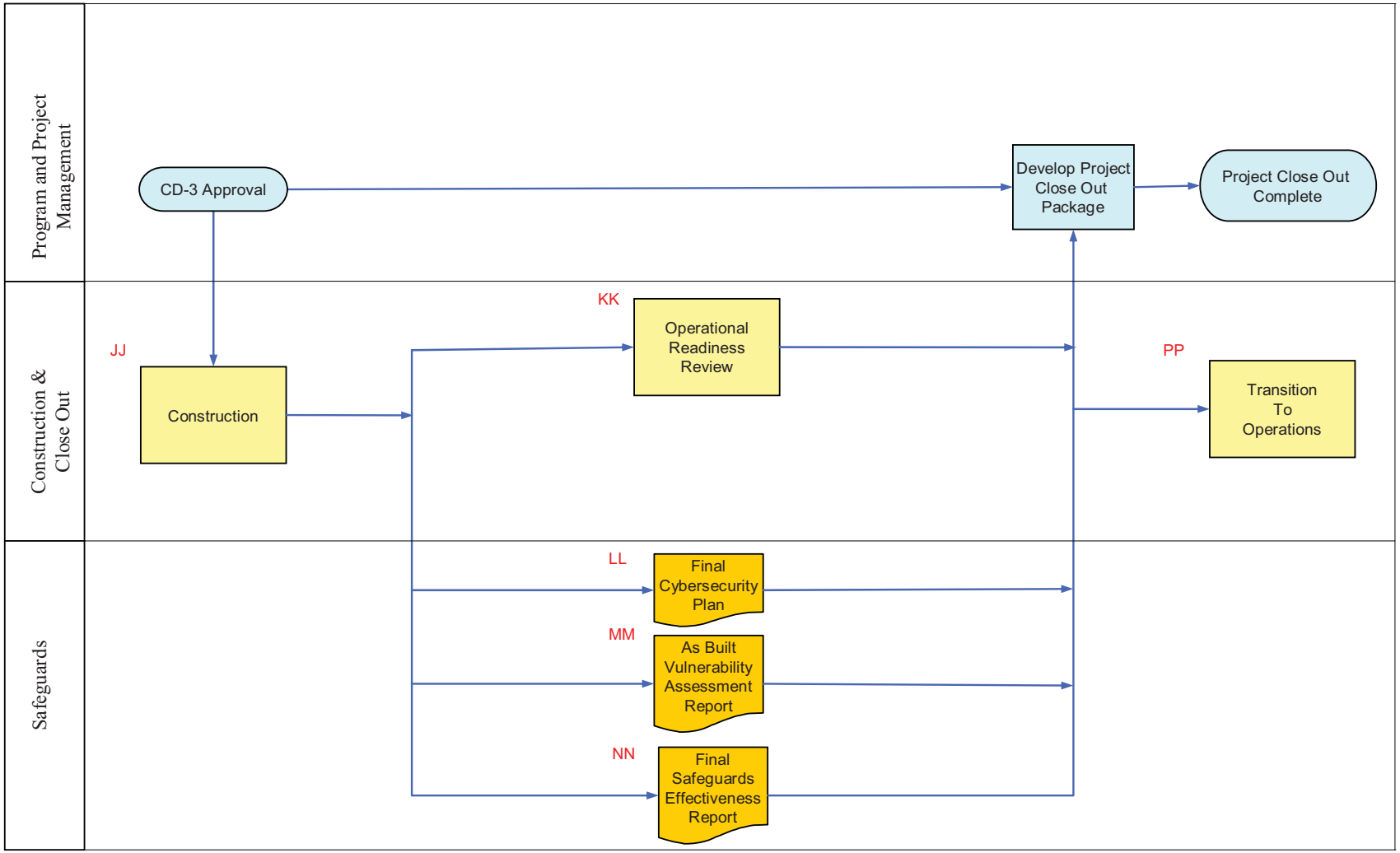


Figure E-5. Safeguards-by-Design process (DOE) – Construction, Transition, Startup, and Closeout.

Letter	Description
II.	For clarity this letter is not used.
JJ.	**Construction** – Construction of the designed facility. Safeguards activities (installation of equipment, verification of design implementation etc.) will be ongoing throughout construction.
KK.	**Operational Readiness Review** – Although titled a review, an Operational Readiness Review is not a project review in the accepted use of the term. Rather, an Operational Readiness Review is an in-depth independent evaluation of the readiness of completed facilities systems equipment procedures personnel and supporting and interfacing systems and organizations to begin facility operation.
LL.	**Final Cybersecurity Plan** – Final update of Cybersecurity Plan as described in "N."
MM.	**As Built Vulnerability Assessment Report** – Vulnerability Assessment Report as described in "M." The level of detail and the particular analyses and tests performed will be appropriate for the facility as constructed.
NN.	**Final Safeguards Effectiveness Report** – Final update to the Safeguards Effectiveness Report as described in "Q" to reflect details of the final design and construction of the facility.
OO.	For clarity this letter is not used.
PP.	**Transition to Operations** – Following successful completion commissioning of plant and a good assessment at the operational readiness review, (ORR) the facility commences normal operational duty.

Note: Greek lettered connector symbols refer to connections between flowcharts in Appendixes E and G.

Appendix F

IAEA Process for International Safeguards

Appendix F
IAEA Process for International Safeguards

F-1. SAFEGUARDS-BY-DESIGN PROCESS INCLUDING INCORPORATION OF IAEA REQUIREMENTS

F-1.1 International (IAEA) Safeguards Considerations

The implementation of safeguards considerations in the design of nuclear facilities follows by extension the U.S. DOE "Safety by Design" process and methodology. The term "safeguards" in this context refers to safety, security, and nuclear material safeguards, both national and international. Whereas most nuclear facility designers are aware of safety and security requirements, regulations, and design issues, this is often not the case for nuclear material safeguards. To promote a better understanding of how the "Safeguards-by-Design" process should incorporate international safeguards issues and requirements, the following section will define these key requirements and propose how they could be efficiently addressed in the process. A key point to note is that international nuclear safeguards requirements must be addressed by all commercial and civilian nuclear facilities. The intention of this report is to describe a process modeled after the U.S. DOE construction project methodology. The DOE environment is one example of what the IAEA calls a State System of Accounting and Control (SSAC). The "Safeguards-by-Design" process is proposed as a new international standard or norm that would be relevant to the design of any new nuclear facility anywhere in the world. The other motivation to including international safeguards considerations in this process is that it is extremely expensive and difficult to incorporate safeguards features and equipment after nuclear facilities begin operation. This is especially so for facilities that will handle plutonium or highly radioactive material. For this reason, the "Safeguards-by-Design" process pays particular attention to identifying the needed activities and their timelines such that all parties have a clear and mutually agreed upon "project plan." [b]

It is important to note that the flow charts that follow define the SBD process for a DOE project and do not reflect desired SBD activities that should take place during the R&D that precedes a project. The authors envisage an IAEA safeguards development process taking place during R&D by nuclear facility vendors. In response to stated goals for safeguardability and proliferation risk reduction (in addition to national safety, safeguards, and security, which are presumably already defined), the designers should try to develop beneficial intrinsic features during early concept development.

F-1.2 The IAEA Safeguards Agreement - The Foundation Safeguards Requirements

Countries that are parties to the "Treaty on the Non-proliferation of Nuclear Weapons" (NPT) are obliged to conclude a safeguards agreement with the International Atomic Energy Agency (IAEA) to safeguard nuclear material within the country and ensure that it is not misused for non-peaceful purposes. This safeguards agreement is typically patterned after the model IAEA comprehensive safeguards agreement in the reference. This agreement establishes requirements for countries and the builder/operators of nuclear facilities that impact the design, start-up and operation of nuclear facilities. This is the case even for countries defined as Nuclear Weapons States (NWS) within the context of this treaty, such as the United States. In countries that are defined under the NPT as "Non-Nuclear Weapons States" (NNWS), i.e., not having exploded a nuclear weapon prior to 1967, the nuclear material and

b. Throughout this section extensive use of IAEA terms is used. These terms are defined in more detail in the IAEA Safeguards Glossary, 2001 Edition, which is available by ordering from the International Atomic Energy Agency, Wagramer Strasse 5, A-1400, Vienna, Austria, or on-line at www.iaea.org.

facilities in the country are to be subject to a comprehensive (or full-scope) safeguards agreement modeled after the IAEA INFCIRC/153 Model Safeguards Agreement. Even countries defined as "Nuclear Weapons States," have Voluntary Offer Agreements, which follow the same requirements as those defined for non-nuclear weapons states. This alignment in requirements was done by the international community so that the rules and regulations for nuclear material safeguards would be comparable in both nuclear weapon and non-nuclear weapon states. The main difference is that international safeguards requirements are implemented at all nuclear facilities under the comprehensive (INFCIRC/153-type agreement), whereas in nuclear weapons states, an Eligible Facility List (EFL) is created by the national nuclear authorities. In the case of the United States, this is compiled by the U.S. Department of Energy and Nuclear Regulatory Commission and is updated and transmitted annually to the IAEA. The EFL for the United States includes all commercial facilities regulated under the NRC and most facilities controlled and regulated by DOE that handle nuclear material. As of 2007, this list included approximately 290 nuclear facilities in the United States. However, nuclear facilities that have a distinct defense mission are excluded from the list. Annually, the IAEA Safeguards Department randomly selects facilities from the EFL for inspection. For the United States as many as five different facilities per year are selected for routine inspection, and these are often rotated the following year. However, it must be remembered that in principle, any facility on the EFL may be selected for safeguards inspection by the IAEA. If the facility is selected, it must be possible to apply IAEA safeguards and meet IAEA safeguards objectives. This is one of the key reasons why the "Safeguards-by-Design" process is stressing international safeguards—so that nuclear facility designers are aware that even in nuclear weapons states, such as the United States, facilities need to be able to meet international (IAEA) safeguards requirements.

Under the IAEA comprehensive (INFIRC/153-type) safeguards agreement the general requirements can be summarized as follows:

Nuclear facilities shall have, utilize, or permit:

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

The important point to note from the above is that all nuclear facilities that are constructed must either meet the stated requirements, or be able to accommodate the nuclear safeguards verification measures and activities noted.

F-1.3 Notification to the IAEA of Facility Construction – As Early as Possible

One of the major findings following the First Gulf War in 1991, after the clandestine uranium-based nuclear weapons program was revealed in Iraq, was that many nuclear facilities had not been previously declared. Subsequent to this discovery, the IAEA Board of Governors resolved that in the future countries that intended to build nuclear facilities should officially notify the IAEA as soon as the decision is made by national authorities to construct, or license the construction of, such facilities. What this means is that in all countries that are non-nuclear weapons states, when the decision is made to build or license the construction of new nuclear facilities, the appropriate national nuclear authority must notify the IAEA before construction begins. This advance notice is intended to give the IAEA adequate time to evaluate the declaration and ultimately determine if the declared facility is as specified and appropriate for the country's nuclear infrastructure. This advance notification also starts the internal process at the IAEA for developing a safeguards approach for the facility. In nuclear weapons states, such as the United States, as soon as a nuclear facility is included on the EFL, this can be interpreted by the IAEA as official notification of the construction of the facility, although the U.S. Mission in Vienna (UNVIE) can also notify authorities at the IAEA directly regarding the decision to construct, or license the construction of, new nuclear facilities. The official notification to construct nuclear facilities in the United States would be made by the U.S. Department of Energy, although the facilities to be constructed may also be under U.S. NRC regulatory control. The official notification by national authorities to construct a nuclear facility is the first key milestone identified in Figure F-1,"IAEA relevant activities in the Safeguards-by-Design Process." Additional flow diagrams depicting this process in more detail are shown as Appendix E, "Flowcharts of Safeguards-by-Design Process for DOE Domestic Regulatory Environment," and Appendix G, "Flowcharts of DOE Safeguards-by-Design Process for DOE Domestic Regulatory Environment with International Safeguards."

F-1.4 Submitting the IAEA Design Information Questionnaire (DIQ)

Under the safeguards agreement between the country and the IAEA, the country is obliged to furnish design information relevant to the design, construction and operation of the nuclear facility for the purpose of adequately safeguarding of the facility. The safeguards agreement states explicit requirements for the submission, evaluation and verification of safeguards relevant facility design information. This design information is provided in a standardized questionnaire and form called an IAEA "Design Information Questionnaire" (DIQ). The purpose of the DIQ is to provide the IAEA with enough information regarding a nuclear facility's function, capacity, process employed, and mode of operation to evaluate the operator's declaration for it to be constructed.

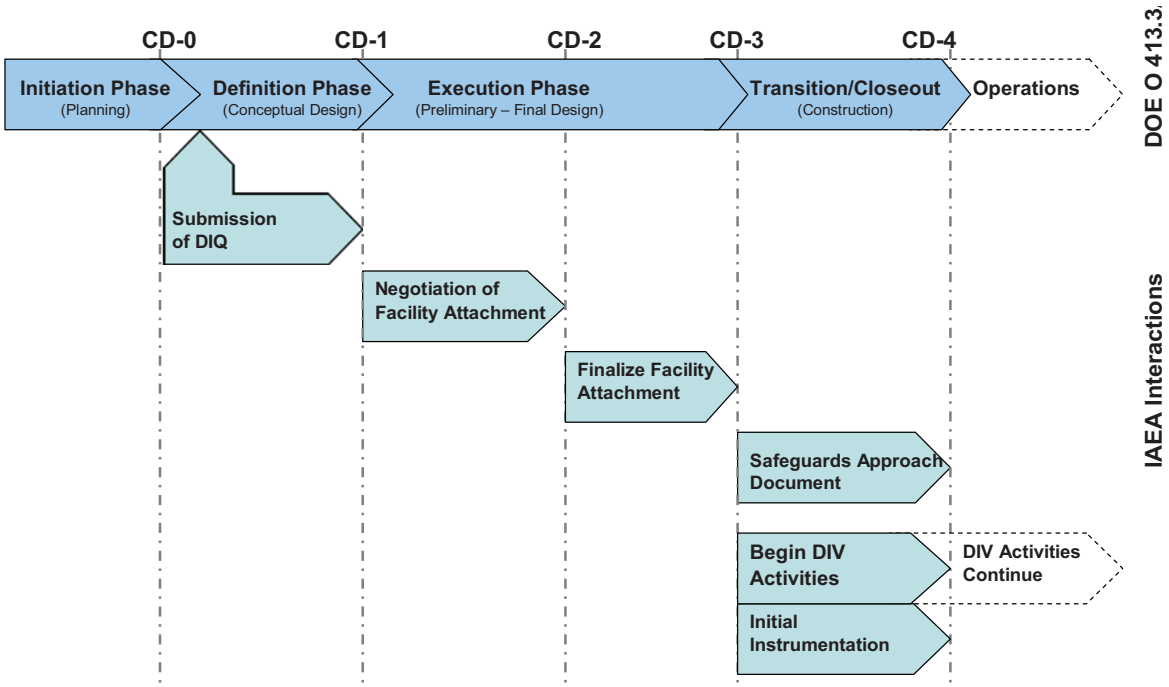


Figure F-1. IAEA relevant activities in the Safeguards-by-Design process.
(IAEA Relevant Milestones are labeled above.)
(DOE Project Design and Construction Stages are labeled above as CD-0, etc.)

The DIQ typically includes the following safeguards relevant design information:

- Name and address of nuclear facility
- Location of, and access to facility, as shown on a regional map
- Type of nuclear facility (i.e., nuclear power plant, etc.)
- Simplified Facility Layout diagram, showing the main nuclear process equipment and nuclear material storage locations
- Type of process, or processes employed for handling nuclear material (i.e., uranium enrichment by gas centrifuge, etc.)
- Simplified process block flow diagram, showing the main nuclear process, or material handling steps
- Capacity of facility or process (i.e., 1000 MWe NPP, or 1000 tonne-SWU enrichment plant, etc.)
- Amounts of safeguarded nuclear material handled – by element and fissile isotope (uranium, U-235, plutonium, etc.)
- Summary of nuclear material measurement and inventory procedures
- Nuclear material flow paths in the facility
- Nuclear material flow paths to and from the facility
- Nuclear material removal routes from within the facility
- Transfer containers, type and capacity, for feeding or removing nuclear material from the facility
- Nuclear waste processes and procedures for assaying waste containers
- Other safeguards relevant design information, as requested by the IAEA.

Model DIQs have been prepared for each major facility type and are available for assisting the nuclear facility operator or designer/constructor in preparing the DIQ, as noted in the reference. For more conventional nuclear facilities, such as nuclear power plants and research reactors, the DIQ is fairly simple. However, the DIQ for nuclear facilities such as uranium enrichment plants, nuclear fuel reprocessing plants, and mixed uranium/plutonium oxide (MOX) fuel conversion or fabrication plants are more complex. For these cases, especially the latter two, the national authorities may need to submit and update facility design information over a period of several years while the facility is being constructed in order to answer all of the IAEA's safeguards relevant queries. The submitting and updating of the IAEA Design Information Questionnaire by national authorities is a major milestone in the Safeguards-by-Design process, shown in Figure F-1.

F-1.5 Verifying Facility Design Information – The IAEA DIE and DIV Activities

After the facility operator or designer/constructor has prepared the IAEA DIQ and submitted it to the national nuclear authorities for forwarding to the IAEA, the IAEA will review the information and schedule follow-up design information verification activities (DIV). The purpose of the DIV is for the IAEA to confirm that the advance declarations regarding the type, size, and purpose for the new nuclear facility are correct and complete. If safeguards-relevant information has not been provided, the IAEA will request additional clarification, and/or information. In performing the DIV, IAEA safeguards inspectors will survey the site from the earliest stages of construction to confirm the location and size of the facility and to determine that the incipient construction is consistent with that facility type. It is important for the future facility operator and the designer/constructor to be aware that the DIV normally starts as soon as excavation for the facility basement and site layout begins. The process of examining the facility design information is called design information examination (DIE).

In accordance with established IAEA Safeguards methodology, DIE and DIV activities are conducted during phases over the entire life of the facility. These phases include: design, construction, cold-testing and commissioning, start-up, operation, shutdown, remodeling, and decommissioning. Once the IAEA is informed by the national authorities of their intention to construct, or license the construction of, a nuclear facility, the relevant IAEA Safeguards Operations Division will begin preparing a DIV Plan for the life of the facility. They will by necessity concentrate on the current design or construction phase of the facility.

It is important to note the DIE and DIV activities performed by the IAEA need to be coordinated by the national authorities with the designer/constructor and operator of the facility. Activities during the construction and start-up stages need to be carefully coordinated with the designer/constructor and operator, because of the numerous hazards during these stages, and to minimize the possible impact on the construction schedule. For large and complex fuel cycle facilities it is also possible that the DIE and DIV activities will reveal safeguards-relevant shortcomings in the current facility design that need to be addressed prior to start-up. This is the main reason why the "Safeguards-by-Design" process notes the interaction with the IAEA during facility design, construction, commissioning, and start-up.

A summary of the verification activities performed by IAEA inspectors during DIE and DIV are listed below by phase in the life of the facility, with emphasis on the early stages of facility design, construction, and startup:

During Conceptual and Initial Design, the IAEA:

- Reviews the DIQ and other relevant design information (DI) at IAEA Headquarters in Vienna and transmits a list of questions regarding any apparent inconsistencies, or about safeguards relevant features.
- Schedules "Design Information Examination" (DIE) activities at the facility with the national regulatory authorities. (It is important that the facility operator arrange a location for this activity

where the facility design information can be secured in locked cabinets and additional information be on hand for clarifying safeguards relevant questions that will be raised).

- May repeat DIE activities at the designer's office or at the facility site during the early stages of site clearing, as required.

The emphasis during this stage is on verifying the completeness of the facility design information provided and the comparison with the advance information provided in the form of the DIQ. During this stage, discussions and negotiations begin between the IAEA, the future facility operator, and national authorities regarding the "Facility Attachment." The Facility Attachment contains specific information regarding the facility, the process employed, the nuclear material handled, the safeguards verification measures to be used, the safeguards instruments and equipment to be used, the verification frequency and accuracy, the estimated number of inspections and inspectors required annually, and any facility-specific methods that will be utilized. More will be said about the Facility Attachment. Discussions regarding the Facility Attachment continue through the construction and testing stages.

During Facility Construction, the IAEA:

- Continues DIE at the facility site during the excavation of the main structures and construction of the facility.
- Performs initial DIV activities, confirming the building size and profile, paying close attention to the possibility of undeclared sub-basements, pipe chases, and other interconnections with ancillary structures on site.
- Measures building dimensions, height, and profile, and confirms that they are as declared.
- Inspects room and cell layout and arrangement during construction and confirms that they are as declared, with emphasis on detecting any undeclared removal routes for nuclear material.
- Begins an initial survey for the placement of safeguards-specific instruments and systems including: surveillance systems, sealing systems, attended and unattended radiation detectors, and/or assay systems, data collection and storage computers and network cable routes.
- Performs a similar survey for the facility operator's systems that may be jointly used for safeguards purposes. (More will be said about the joint-use of operator's instruments for safeguards purposes below).

The emphasis during this stage is on confirming that the facility being constructed is consistent with the type, size and purpose of the nuclear facility as conveyed by the national regulatory authorities in the DIQ. This is also the most important stage for facility access, since later large parts of the facility may be inaccessible during operation, due to radiation or other safety hazards. This stage is also important, because it allows IAEA inspectors the first real glimpse into where the key safeguards-specific equipment and systems will be located. During this stage particular attention is also paid to potential removal paths and storage locations for nuclear material. This stage is also important, because at this point the complete network of safeguards equipment, systems, data collection, and computing equipment, and their connections with the process are easier to visualize and assess.

During Cold-testing, Commissioning, and Start-up, the IAEA:

- Participates in, and witnesses the calibration of safeguards relevant plant instruments.
- Inspects the placement of, and tests IAEA safeguards specific surveillance systems, seal systems, unattended and attended radiation detectors and assay systems, data collection and transmission systems.
- Calibrates IAEA safeguards-specific unattended and attended radiation detectors and assay systems.

- Continues to perform DIE and DIV activities, especially on important safeguards-relevant features in the facility.
- Performs dry-runs and tests of safeguards equipment, methods, and procedures, and evaluates their initial performance with a view towards actual operation.

This stage is especially important, because it is at this point that most of the systems are finally fully interconnected. At this stage the quality and completeness of the design become most apparent. Similarly, it is also at this time that the complete functional interconnection of the safeguards equipment and systems is made and tested. Also, this is the first time when the safeguards methods and procedures can be dry-run and tested. This allows the IAEA, the facility operator, and the national authorities an initial opportunity to assess the safeguards equipment, methods and procedures.

F-1.6 Facility Specific Safeguards Requirements – The IAEA Safeguards Criteria

Safeguards inspection criteria have been developed and codified by the IAEA based on the type of nuclear facility, (e.g., nuclear power plant, research reactor, uranium conversion plant, uranium enrichment plant, etc.) and are summarized in the Safeguards Criteria Section of the *IAEA Safeguards Manual*. These criteria specify the facility safeguards requirements additional to those in the Safeguards Agreement. The safeguards requirements depend on the type of nuclear material (low enriched uranium [LEU], highly-enriched uranium [HEU], plutonium and thorium), and whether the material is irradiated or un-irradiated. The criteria are more stringent for what the IAEA calls "Direct Use Material"—material which, if diverted, could be potentially processed to produce a nuclear weapon. For Direct Use Material, the specified verification frequency, measurement accuracy, and detection probability is higher.

For each type of nuclear facility, the Safeguards Criteria specifies requirements for:

- Examination of safeguards relevant operating records and state reports
- Performing annual Physical Inventory Taking (PIT) and Verification (PIV)
- Verification of domestic and international transfers of nuclear material
- Verification of other nuclear inventory changes
- Verification of nuclear material flow at "Other Strategic Points" (OSP)
- Confirmation of non-production of Direct Use Material
- Confirmation of the absence of borrowing of nuclear material between facilities or MBAs
- Performing nuclear Material Balance Evaluation
- Verification activities at Interim Inspections (IIV) for timely detection of diversion
- Verification of and follow-up for safeguards "Discrepancies" or "Anomalies"
- Verification of facility "Design Information" (DIV)
- Verification of the facility operator's measurement systems (used for safeguards)
- Confirmation of nuclear material transfers
- Verification activities related to partial attainment of IAEA inspection goals
- Verification related to non-nuclear material under safeguards (i.e., heavy water)
- Verification activities related to equipment and facilities under safeguards
- Activities for the preparation of inventories of nuclear material, equipment, and facilities.

These facility-specific requirements 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, especially if the designer is unfamiliar with international safeguards requirements. The challenge in reading and interpreting the IAEA Safeguards Criteria and the Safeguards Agreement is that they are written in a kind of legalese with extensive use of IAEA-specific terms. As noted earlier, the use of the *IAEA Safeguards Glossary* is helpful for interpreting the meaning of the specified requirements. However, the best solution is the involvement of IAEA Safeguards staff, former IAEA staff and other national safeguards experts to interpret the criteria and specified safeguards verification requirements. This is a key element in the "Safeguards-by-Design" process—the early involvement of international safeguards experts during the design, construction and start-up of new nuclear facilities to ensure that the facilities and nuclear material therein can be adequately safeguarded.

Ultimately, it is envisioned that the development of a "Safeguards Best Design Practices" guide could capture the established safeguards design practices and solutions that have been implemented to address these safeguards verification requirements. These "Best Practices" would catalogue the specific requirement and manner in which the safeguards issue was addressed. Even though the implementation of international safeguards varies to some degree individually from facility to facility, the fundamental safeguards requirements, especially for nuclear facilities of a given type, remain the same.

The "Facility Attachment" also has a bearing on the design of the facility, with emphasis on equipment and design features unique to the particular facility. This discussion follows below.

F-1.7 The Facility Attachment and its Relevance to the "Safeguards-by-Design" Process

After submitting the initial DIQ, the national authorities, facility operator, and the IAEA begin discussing and negotiating the "Subsidiary Arrangements" (to the safeguards agreement), relevant to the facility being constructed. The Subsidiary Arrangements consist of a General Part, applicable to all common nuclear activities of the country, and a "Facility Attachment," prepared for each facility in the country and describing safeguard arrangements specific for that facility. The Facility Attachment describes in detail what inspection activities will be performed in the facility, the instruments to be used (both operator and inspector), the frequency of inspections, and estimated level of inspection effort. Since these are facility specific, they must be negotiated between the IAEA, the national authorities, and the builder/operator of the facility while the facility is being designed and constructed. Even though the national authorities and builder/operator of the nuclear facility have significant input into the Facility Attachment, the IAEA must approve it, since it will dictate whether IAEA safeguards can or cannot be practically implemented at the specific facility. Not addressing these issues at an early stage in the process may result in the construction of a facility in which international (IAEA) safeguards cannot be implemented. This could have serious consequences and political ramifications for a country that is a declared party to the NPT. As noted above, the Facility Attachment is dynamic and evolves during the design, construction, and testing of the facility. In principle, it captures the facility-specific issues relevant to safeguarding the facility and implementing the IAEA's "Safeguards Approach," which is described in more detail below. Discussions regarding the Facility Attachment continue through the cold-testing and commissioning stages. However, the Facility Attachment must be finalized and agreed between the facility operator, national authorities, and the IAEA Safeguards Department prior to start-up and operation of the facility. Model Facility Attachments for different types of facilities are available from the IAEA Department of Safeguards.

F-1.8 The Facility Safeguards Approach and its Relevance to the "Safeguards-by-Design" Process

The IAEA "Safeguards Approach" describes the specific safeguards verification and accountancy measures that will be implemented at the facility to meet the IAEA safeguards inspection goal. This goal is to detect, with a high level of confidence, the diversion of one "Significant Quantity" (SQ) of safeguarded nuclear material within a period for timely detection.[c] The Safeguards Approach is prepared and approved exclusively by the IAEA. It is not an external document, nor is it approved by the national authorities. However, the Safeguards Approach depends on the Facility Attachment, which does permit the national authorities and facility builder/operator an opportunity for ensuring that the Safeguards Approach will not be excessively burdensome, inefficient, or inappropriate for the facility being constructed. The Safeguards Approach is based on the "Safeguards Criteria" and requirements noted in the IAEA Safeguards Manual. However, the IAEA may customize the safeguards approach for implementing safeguards on a site or state-level, depending on the circumstances for the particular country. What is relevant to this discussion is that the Safeguards Approach should be completed and approved by the IAEA before the facility operates – although the onus for this is more upon the IAEA than the national authorities or facility builder/operator.

F-1.9 Joint Use of Instruments with the IAEA for Safeguards Purposes – The Potential Impact on Facility Design

For large and complex nuclear cycle facilities, it is becoming more common to use the facility operator's instruments for process control, as a complement to the IAEA safeguards-specific instruments. This is especially so for large-scale nuclear fuel reprocessing plants, as was recommended in the final report of the Large Scale Reprocessing Plant Exercise (LASCAR), jointly conducted by the IAEA and member states. Analogously, the idea of sharing instruments with the plant operator is probably also relevant to the case of safeguarding MOX conversion, MOX fuel fabrication, and potentially to uranium enrichment plants. The apparent benefits are that the facility operator has a vast array of precise instruments, many of which are on-line providing data in real-time, throughout the facility. Joint use of some of these key instruments would give the IAEA inspectors a benefit of scale and additional instruments for complementing and/or corroborating IAEA safeguards data. However, the IAEA Safeguards Department has a fairly restrictive policy regarding the sharing of joint-use instruments for safeguards purposes with another party. The policy establishes that it is possible for the IAEA to jointly share instruments with either the national authorities or the facility operator, provided that the IAEA is able to make independent safeguards conclusions from the instrument.

Key points from the IAEA Safeguards/SGTS Policy #20 are as follows:

- Each case of joint use of instruments for safeguards purposes between the IAEA and another party must be approved by the Deputy Director General of Safeguards (DDG/SG - the head of the IAEA Safeguards Department)
- When changes or modifications are made to joint use instruments, the applicability of joint use must be reviewed by a Technical Review Committee in the IAEA and will require re-approval by the DDG/SG
- In principle, the IAEA discourages the joint use of safeguards instruments with another party to protect the independence of the IAEA safeguards findings or conclusions

---

c. For low enriched uranium (as in the form of fresh nuclear fuel or UF6), the Significant Quantity (SQ) is defined by the IAEA as 75 kg of U-235, the diversion of which is to be detected within one year. For un-irradiated plutonium (as in the form of MOX), the Significant Quantity is 8 kg of Pu to be detected within one month. For irradiated plutonium (as in the form of spent fuel), the Significant Quantity is 8 kg Pu to be detected within three months of possible diversion.

- It is possible for the IAEA to jointly use instruments for safeguards purposes with the national authorities or facility operator, provided that this is more economical than using independent equipment, and provided that the IAEA can draw independent conclusions from the jointly used instrument.

In other words, the construction of large complex nuclear fuel cycle facilities tends to drive the joint use of instruments for safeguards purposes between the IAEA and the national authorities or facility operator. However, each case must be reviewed by the IAEA and may be rejected if the IAEA determines that the sharing of instruments could affect the independence of its safeguards conclusion. This issue is especially important and is called out explicitly in this discussion on the "Safeguards-by-Design" process, because it implies that a large and complex facility to be safeguarded by the IAEA will probably require either a provision for the installation of separate IAEA safeguards equipment, or the actual installation of such equipment, prior to facility start-up. Discussions continue at the IAEA, regarding the degree of independence that must be achieved. It has also been suggested that if the IAEA still has enough key stand-alone instruments, it may be possible to jointly use the operator's instruments in a complementary manner, rather than to derive primary safeguards conclusions. In any event, this discussion is current and on-going. More will be said regarding the joint-use of particular safeguards instruments and the impact on the facility operator and facility design at the newly constructed Rokkasho-mura Reprocessing Plant (RRP) in Japan in the section below.

The key point is that the national authorities and/or facility operator should not assume that the IAEA will simply use the other's safeguards instruments for the sake of deriving its safeguards conclusions. The IAEA is likely to require the installation of at least some independent instruments for this purpose. These instruments need to be anticipated and accommodated by the facility designer and would need to have at least space and requisite utilities provided during facility construction. Depending on access limitations, the placement and installation of IAEA safeguards equipment may be required during the start-up and commissioning phase of the project—but probably prior to start-up of the facility in many cases. The best way to determine what would be required would be to discuss the matter with the IAEA Safeguards Department during the design phase of the project.

F-1.10 Safeguards-by-Design: Lessons Learned from the Rokkasho-mura Reprocessing Plant Project

The Rokkasho-mura Reprocessing Plant is a commercial large-scale reprocessing plant, which was constructed in northern Japan from the 1996 until 2006, when cold-testing and commissioning began. This project is a very important point of reference for the proposed "Safeguards-by-Design" process, because elements of this process were incorporated into this construction project. This facility is the first large-scale reprocessing plant subject to comprehensive IAEA safeguards and routine inspection from head-end to tail-end, and it was also a very large and complex facility and safeguards undertaking. The Japanese national authorities (JAEB/JSGO) notified the IAEA of its intention to license the construction of a large-scale commercial reprocessing plant in the late 1980s. This inspired the IAEA to involve a number of member states in the aforementioned Large-Scale Reprocessing Plant Exercise (LASCAR). Because the Japanese authorities notified the IAEA at such an early stage, it led to very good communication between the national authorities (JAEB/JSGO), the facility owner operator (JNFL) , and the IAEA Safeguards Division of Operations-A (with responsibility for safeguarding Asia). Actual coordination of the DIE, DIV, safeguards construction, and routine inspection activities was managed by the JNFL Project Group within the Division of SGOA at the IAEA.

The major steps involving the IAEA in the proposed "Safeguards-by-Design" process were demonstrated in this project, including:

- Early notification by the national authorities of their intention to construct a new nuclear facility.

- Submission by the national authorities of a detailed DIQ, which was regularly updated over the course of the design, construction and testing phases of the project.
- Early, extensive, and well-coordinated safeguards dialog with the IAEA (JNFL Project Team). This included placing a liaison for JNFL at the IAEA and identifying a liaison in the IAEA Tokyo Regional Office to facilitate communication back and forth.
- Well-coordinated and regular DIE and DIV activities, which began at the earliest stages of conceptual design in Tokyo in 1996, and which moved to the construction site once site clearing and excavation began.
- Regular and well coordinated dialogue between JAEB/JSGO, JNFL and the IAEA regarding the development of the Facility Attachment.
- Input from JAEB/JSGO and JNFL into the IAEA Safeguards Approach for the facility.
- Well-coordinated support for IAEA installed and joint-use safeguards relevant instruments, during the cold-test and commissioning stages of the project.
- Well coordinated involvement of the IAEA in the calibration of the vessel level and density instruments for vessels of safeguards relevance. This allowed the IAEA the opportunity to witness and partake in the actual process vessel calibration activities – which took years to complete.
- Extensive back and forth dialog regarding proposed safeguards measures, joint-use of instruments for safeguards purposes, and additional encryption or data authentication for specific safeguards systems.

The point of this is to note for the record that IAEA involvement in the Rokkasho-mura Reprocessing Plant project was essentially a successful example of the proposed "Safeguards-by-Design" process. The major steps and milestones in this project have now been codified in the "Safeguards-by-Design" process. From this experience, the benefits of early involvement by the IAEA in the project, and extensive and active safeguards dialog between the national authorities, facility operator and the IAEA have been clearly demonstrated. The absence of this early involvement, or lack of active and energetic safeguards dialog, is not something to be analyzed by a cost benefit analysis. Without these, the construction of such a large-scale fuel cycle facility would lead to something which cannot be adequately safeguarded. That is the fundamental motivation for the "Safeguards-by-Design" process—to avoid that outcome.

More facility specific points, lessons learned, and a short-list of proposed "Best Practices" from the Rokkasho Reprocessing Plant project are summarized in the Appendices D.4 and H.2.

F-1.11 Safeguards Best Design Practices – Harvesting the Best "Prior Art" to Guide Effective Safeguards in the Design of Future Facilities

As was noted earlier in this chapter, there are a number of international safeguards regulations, requirements and criteria which must be considered in the design of new nuclear facilities. These regulations and requirements are based principally on the Safeguards Agreement between the country and the IAEA and the IAEA Safeguards Criteria, with additional requirements from the Facility Attachment and the IAEA Safeguards Approach. The challenge to the facility designer and constructors is in understanding these requirements, since they are typically presented in IAEA-specific legalese.

To facilitate the understanding of these requirements, the authors envision the preparation of a set of "Best Safeguards Design Practices." These could be prepared in the manner of the current IAEA Safeguards Criteria in the *IAEA Safeguards Manual* and arranged and listed by facility type (i.e., nuclear power plants, research reactors, uranium conversion plants, etc.). The Best Practices would list the relevant requirement, either in the original language, or paraphrased in a more easily understood form. It would then list the specific safeguards equipment or method that has been successfully used to address the

requirement, together with references to the origin of the requirement, as well more details regarding the proposed best practice. Examples of Best Practice sketches are shown in the Appendix H. However, it should be noted that these emphasize spent fuel reprocessing and MOX fuel fabrication facilities and are quick sketches.

In reality, “Safeguards Best Design Practices” need to be developed for each facility type, with a strong connection to the fundamental or referenced requirements. These would need to be on a level of detail consistent with existing regulations and design practices as codified in the American National Fire Code, National Electrical Code, and other existing codes for electrical, mechanical, fire, chemical and nuclear safety. Only then would facility designers have a clear idea of how to systematically address the safeguards requirements.

The application of SBD with fully mature requirements and design methodology at some time in the future may well only use best practices as a starting point and guide. The ultimate objective is to evolve new, improved, intrinsic design features, which may be quite different than existing approaches, for safeguardability.

APPENDIX G

Flowcharts of Safeguards-by-Design Process for DOE Domestic Regulatory Environment with International Safeguards

APPENDIX G

Flowcharts of Safeguards-by-Design Process for DOE Domestic Regulatory Environment with International Safeguards

G-1. SBD FLOWCHARTS FOR INCORPORATION OF IAEA REQUIREMENTS

The SBD process is a systematic and structured series of steps directed to fully integrating international and national safeguards, physical security, and other proliferation barriers into the design and construction process for nuclear facilities, with the objective of increasing the safeguardability, protectability, and proliferations resistance of facilities. As explained in Volume 1, Section 3.1, the optioneering study generated a single process covering domestic and international (IAEA) safeguards. However, the study was performed in two stages: first, a process was developed using DOE domestic requirements and SBD team's performance requirements only, see Volume 1, Section 3.2, and second, the first results were modified to integrate the additional effects of incorporating international (IAEA) requirements, see Volume 1, Section 3.3. The step-wise approach was to simplify the study and facilitate its visual representation by means of two series of flowcharts, Appendix E (domestic environment) and the present appendix (domestic environment and international safeguards).

Each of the following flowcharts outlines the SBD process in the DOE facility acquisition process; each design phase ends with the successful completion of a critical decision point. The DOE critical decision points are process checkpoints that specify that specific requirements that are needed to be met and approved to continue with subsequent steps in the design process. The flowcharts show three distinct levels that demonstrate the interactions between State activities (initiated by the Safeguards-by-Design Team (SBDT)), Project Engineering, and Program and Project Management. The Program and Project Management group operates as project leadership. The Project Engineering group uses the guidance provided by the Program and Project Management group and further manages the project by interacting with the SBDT. A fuller textual discussion of the SBD process is given in Volume 1, Section 3. The SBD process uses the basic process flow charts originated for Safety-in-Design as provided in DOE STD-1189-2008, March 2008, Integration of Safety into the Design Process.

The following flowcharts, Figures G-1 through G-4, are closely related to Figures E-2 through E-5 with additional information regarding incorporation of actions to meet requirements for the IAEA. The figures, as previously discussed, are broken down into design phases, which show the order of interactions between the international and domestic process steps. The darker shade boxes show the actual action, deliverable, or interaction point between the IAEA and the DOE. In the case of RR', the lighter shade boxes with dashed borders designate a preferred early appearance before the mandated appearance in the following critical decision point, which means that these requirements should be completed as early as possible.

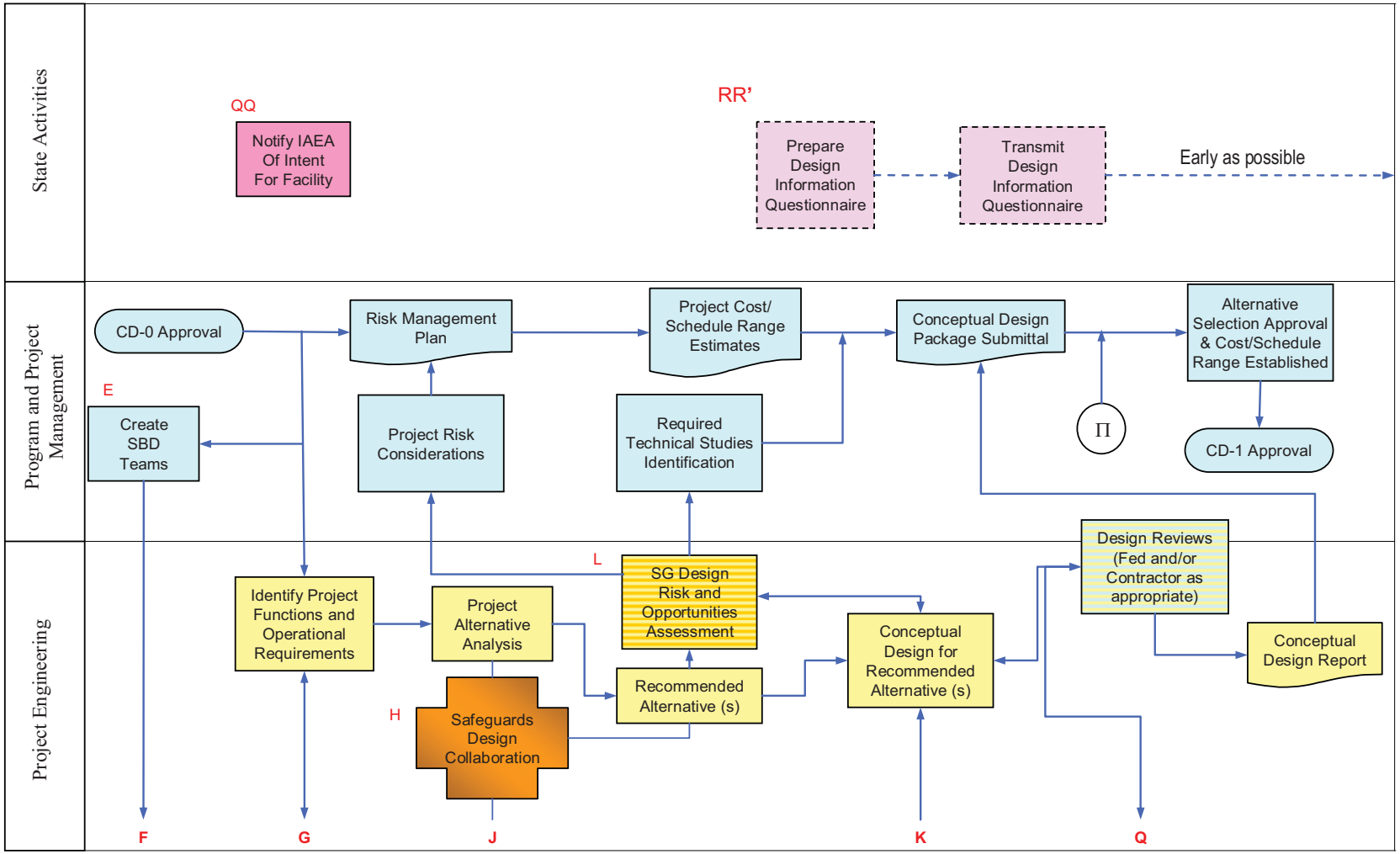


Figure G-1. IAEA interfaces with safeguards-by-design process (DOE) – Definition Phase.

Letter	Description
QQ.	**Notify IAEA of Intent for Facility** – Intrinsic features that are necessary to allow proper IAEA verification must be considered and included, as necessary, early in the design process to avoid costly redesign and retrofit efforts. Early notification to the IAEA, to allow the international processes to begin is crucial. Additionally, for NWS, such as the United States, determination of whether to place the facility on the Eligible Facilities List must occur early to allow the rest of the process to go forward in a timely fashion.
RR'.	**"RR"** – The DOE project management process, M 413.3-1, establishes the preferred design alternative for the facility by the time of CD-1 approval. Standard 1189-2008 emphasizes the importance of establishing the facility arrangement by no later than CD-1. This means there is significant time pressure to make the IAEA interaction support this schedule – particularly insofar as major facility alternatives and infrastructure needs are concerned. Conversely, RR may move more into the CD-1 phase as shown on 4-5.

Note: Greek lettered connector symbols refer to connections between flowcharts in Appendixes E and G.

.

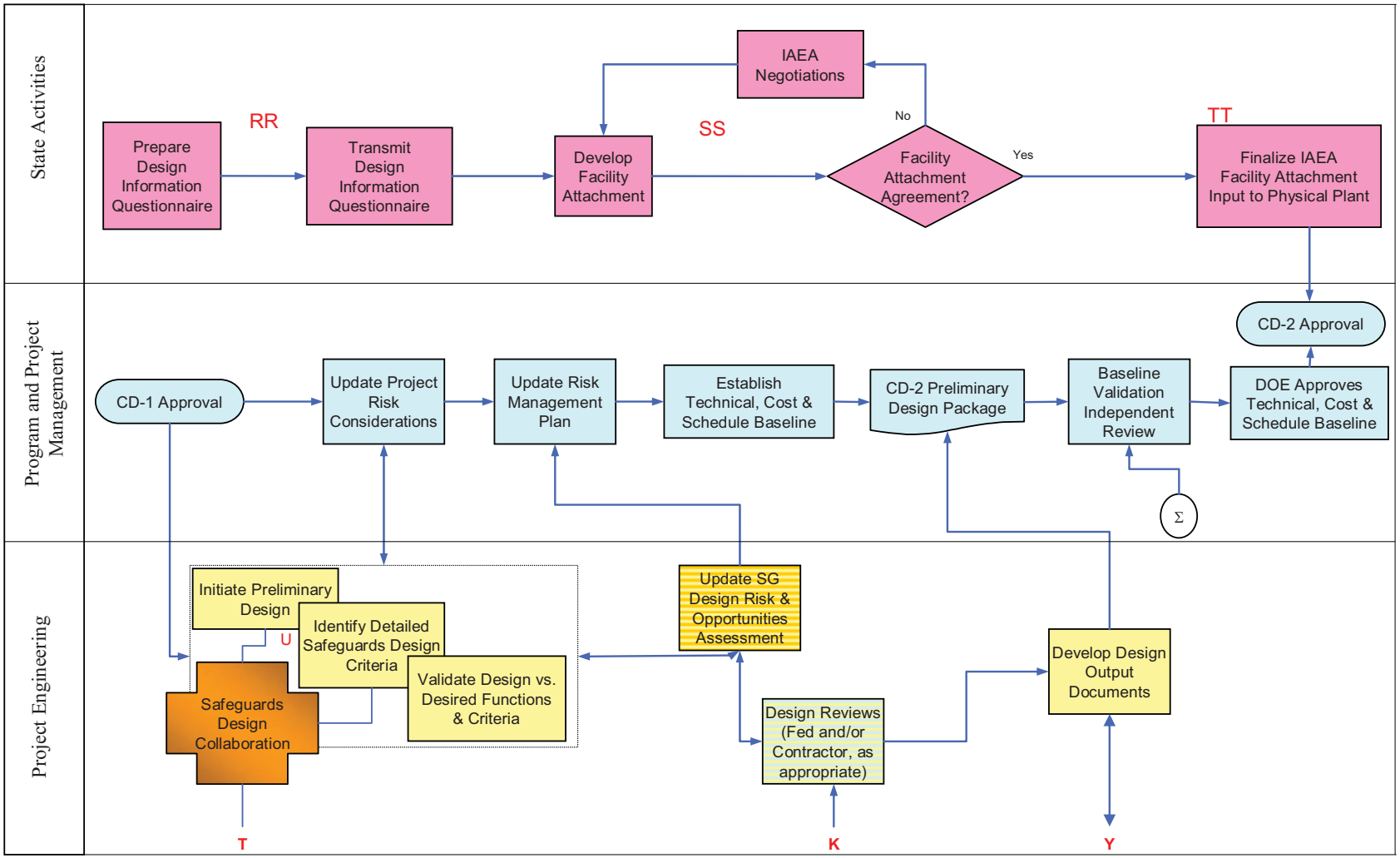


Figure G-2. IAEA interfaces with safeguards-by-design process (DOE) – Preliminary Phase.

Letter	Description
RR.	**Prepare and Transmit Design Information Questionnaire (DIQ)** – The IAEA involvement currently begins in earnest with the DIQ. Preparation of the DIQ requires that a minimal amount of the design has been completed, thus this action is current immediately after the completion of the conceptual design phase. Transmittal of the DIQ to the IAEA requires coordination between the design team, national regulatory agencies (e.g., DOE), and state-level organizations (e.g., U.S. State Department).
SS.	**Facility Attachment** – The facility attachment is a negotiated document between the IAEA and the state regarding the features (intrinsic and extrinsic) that will be incorporated into the facility design to accommodate the IAEA verification activities during construction and operation.
TT.	**Finalize IAEA Facility Attachment to Physical Plant** – It is vital that the impact of the facility attachment on the physical plant (lab space, conduits, footprint of hot cells, IAEA instrument space, Inspector office, etc.) be agreed upon in a timely fashion to allow the detailed design efforts to proceed.

Note: Greek lettered connector symbols refer to connections between flowcharts in Appendixes E and G.

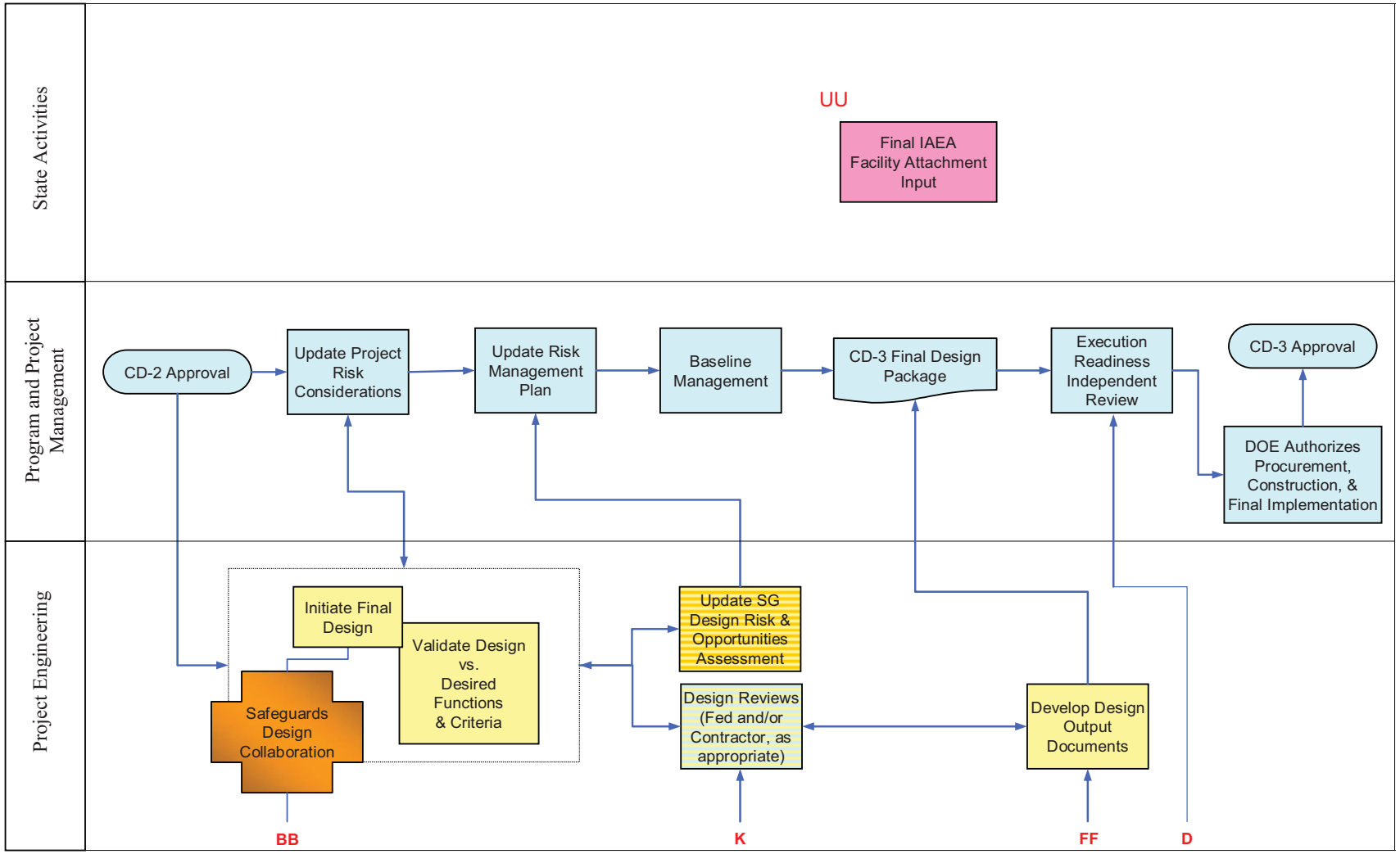


Figure G-3. IAEA interfaces with safeguards-by-design process (DOE) – Execution Phase, Final Design.

Letter	Description
UU.	**Finalize IAEA Facility Attachment Input** – As the design effort progresses to finer detail, so also does the IAEA facility attachment input. As the facility design is optimized and reviewed for final approval, the IAEA input is finalized and incorporated into the overall design.
PRD.	**Program Requirements Document** – DOE NNSA requires the submission of a Program Requirements Document (PRD) for Construction programs/projects being executed by NNSA. It translates the "need" in the Mission Need Statement into initial top-level requirements addressing such concerns as performance, supportability, physical and functional integration, human integration, security, test and evaluation, implementation and transition, quality assurance, and configuration management. (NNSA Policy Letter BOP-50.004, 02-15-2008)

Note: Greek lettered connector symbols refer to connections between flowcharts in Appendixes E and G.

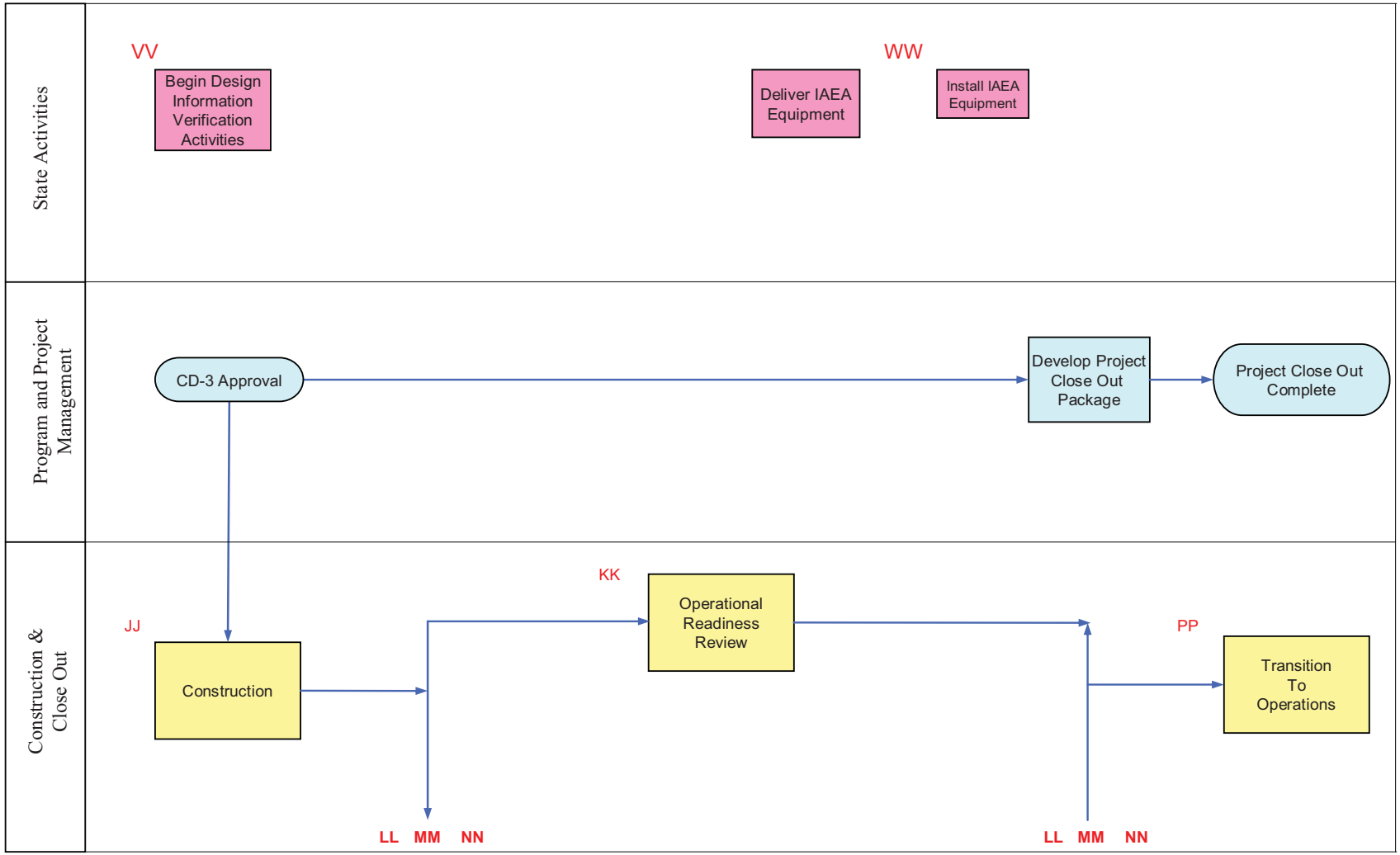


Figure G-4. IAEA interfaces with safeguards-by-design process (DOE) – Construction, Transition, Startup, and Closeout.

Letter	Description
VV.	**Begin Design Information Verification (DIV) Activities** – As construction begins, DIV activities will be performed by the IAEA through all stages of construction and will continue as needed during operation.
WW.	**Deliver and Install IAEA Equipment** – As the facility is built and prepared for operation, the IAEA equipment needs to be delivered and installed (including testing, tamper-proofing, initial calibrations, etc.)

Note: Greek lettered connector symbols refer to connections between flowcharts in Appendixes E and G.

The SBD process has identified interaction points and deliverables required within the IAEA process affecting the U.S. facility design and construction. These include submission of the DIQ to IAEA, negotiation of the Facility Attachment (covering design to commissioning), preparation by IAEA of the Safeguards Approach document, DIV including optional inspections by IAEA. Information on IAEA requirements for international safeguards including inventories, quantities, and deviations is given in Appendixes D and F. These opportunity points allow the IAEA to increase the effectiveness of facilities' safeguards and integrate their systems into the design of facilities since it is important, at the key interaction points, that the IAEA offers timely input. A fuller textual discussion of the SBD process incorporating both domestic and international requirements is given in Volume 1, Section 3.

Appendix H

Applying Best Practices and Lessons Learned to Institutionalizing Safeguards-by-Design

Appendix H
Applying Best Practices and Lessons Learned to ISBD

H-1. INTRODUCTION

A "Best Practice" is a process, practice, or system identified in public and/or private organizations that performs exceptionally well and is widely recognized as improving the performance and efficiency of organizations in specific areas. Best practices are likely to be innovative, make a difference, have a sustainable effect and have the potential to be replicated and to serve as models for generating initiatives elsewhere. Successfully identifying and applying best practices can reduce costs and improve organizational efficiency. Best practices may be identified through assessment of, ideally many, organizations to develop excellence benchmarks. Typically, best practices are positive activities or systems that one recommends to others for use in similar situations.

A "Lesson Learned" documents the experience gained from working with or solving real-world problems, for example, during a project. A lesson learned identifies problems and how to solve them. Collecting and disseminating lessons learned helps to eliminate the occurrence of the same problems in future projects. Lessons learned typically are negative with respect to identifying process, practice, or systems to avoid in specific situations. Lessons learned are positive with respect to identification of solutions to problems when they occur. Lessons learned may be distinct to an individual organization, specific program or project and are not necessarily universal in scope or application. They may be lessons from events, which have severe negative consequences to stakeholders and perhaps attract adverse publicity. Despite their infrequent occurrence, they may offer extreme examples of how not to do something, which become well known throughout an industry, country or world-level and have considerable impact.

It is normal practice to document accumulated best practices and lessons learned in written form so that they remain accessible and the evolution of know-how with new requirements, discoveries and developing maturity can be perceived through an iterative approach. Many organizations now operate knowledge management systems incorporating best-practice and lesson-learned data.

The Office of Health, Safety and Security in U.S. DOE operates a Corporate Operating Experience Program, which helps to prevent the recurrence of significant adverse events/trends by sharing performance information, lessons learned and good practices across the DOE complex. This program includes:

1. DOE Site Performance Information
2. ORPS Weekly Summary of Significant Occurrences
3. DOE Corporate Lessons Learned Collection - Jump to the Lessons Learned products, http://www.hss.energy.gov/csa/analysis/ll/ (October 2, 2007).

Lessons Learned Resources Applicable to DOE Users include:

1. Defense Nuclear Security Lessons Learned Center
2. Energy Facilities Contractor Group Best Practices
3. DOE Society for Effective Lessons Learned Sharing.

There are also links to other lessons-learned and best-practice resources, which are grouped in the following major categories:

- DOE Sources: Links to DOE Headquarters Lessons Learned web pages, and DOE Field Lessons Learned pages (web pages from DOE sites).

- Non-DOE Sources: Links to Other Government Agencies web pages including those of military services and links to commercial, professional and other non-governmental organizations.

In the remainder of this appendix, four examples of best practice and one of lessons learned are summarized for application to the ISBD framework and SBD process. The four best practices are taken from the development leading to the safeguards system for Rokkasho-mura oxide fuel reprocessing plant in Japan, the design and construction of the Mixed Oxide Fuel Fabrication Facility, now being built at the Savannah River Site in South Carolina to convert surplus weapons plutonium into MOX fuel for use in commercial reactors, the development of unclassified safeguards requirements documents, and the broad issue of how the focus of integration of safeguards has evolved over decades. The lesson learned is, the THORP, Sellafield, UK oxide reprocessing plant prolonged HA liquor leakage to the feed clarification cell. These diverse, real-world examples important to nuclear fuel cycle facility design, construction and operation were selected to show successes, failures and diverse previous efforts against which the ISBD framework and the SBD process was tested and which informed the ISBD Project Team.

H-2. BEST PRACTICE – IAEA SAFEGUARDS FOR ROKKASHO-MURA REPROCESSING PLANT

H-2.1 Early IAEA Experience

This section summarizes IAEA experience with safeguarding reprocessing plants commencing in the late 1960s and developing towards the current best practice as epitomized by IAEA collaboration with Japan in deployment of safeguards at the Rokkasho-mura Reprocessing Plant (RRP), which represents the state-of-the-art PUREX thermal oxide fuel recycling facility worldwide.

The relevant points learned from the IAEA started in 1969 with the first IAEA inspection of a reprocessing plant at West Valley, New York. At the time, safeguards methodology was only emerging and the inspection was limited to simply observing the measurements by the operator and independently recording the data by the IAEA inspectors. The inspection was limited in duration to the processing of a single campaign of fuel from a single reactor. The inspectors were in residence near the facility and on-call to be present during important measurements. Measurement capabilities were quite rudimentary. Non-destructive analysis development was in its infancy. Volume measurements used water manometers. Mass spectrometry was the method for input and product measurement and waste measurements were by alpha counting, requiring “assumptions” in isotopic composition based on input analyses.

At the time, West Valley was the only significant commercial plant in operation in the U.S. It was run in short fuel campaigns with plant cleanout and inventory between each campaign so frequent material balance could be evaluated. The only other plant was in Mol, Belgium, but this was a much smaller facility. There were other reprocessing plants in operation but some were associated with weapons programs and not fully subject to IAEA inspection. Subsequent to West Valley, there were limited inspection activities in Germany at the Karlsruhe facility, but again, this was a very small facility. The French were operating the initial reprocessing facility UP-2, but this was not subject to extensive IAEA safeguards being in a weapons country and the UK was operating the B205 Magnox reprocessing facility, which mainly processed commercial gas-reactor metallic fuel but also conducted campaigns of defense related fuels.

By the late 1970s, the U.S. had built the Barnwell Nuclear Fuel Plant, which was the first of the next generation of large-scale facilities with a capacity of 5 ton/day, with continuous operation for 200-250 days per year. There was considerable development of safeguards measurement and evaluation technology at Barnwell through the later 1970s, with interactions with the IAEA for planned inspection activities, even though the plant never operated with irradiated fuel. But with the change of U.S. policies towards plutonium recycle in 1977, it became apparent the IAEA would not be challenged by safeguards at this large scale facility.

It was not until the late 1970s that the IAEA was faced with the new challenge for inspection of the Tokai Reprocessing Facility in Japan. This facility could also be considered a pilot facility for commercial operations, contemporary with West Valley and the French UP-2 plant, built largely with design assistance from France. The IAEA became involved late in the commissioning phase. It presented a new challenge to the international safeguards community, as it was the first significant facility in a non-weapons state, and was planned for continuous operations over periods longer that the time intervals for IAEA detection goal objectives. The Tokai Advanced Safeguards technology Exercise (TASTEX) was the safeguards Technology improvements program for the Tokai Reprocessing Plant (TRP) in cooperation with four parties, i.e., Japan, the United States, France and the IAEA. The exercise with 13 tasks was initiated in February 1978 and ended in May 1981. It assisted the IAEA with development and implementation of safeguards techniques to meet the challenges of continuous inspection in this 0.7 ton/day facility. Another initiative was the Hexapartite Safeguards Project (HSP) in 1980.

The TASTEX experiment implemented a number of significant new ideas, among which were:

- Use of electromanometers for volume measurement displacing the contemporary water manometers
- Use of resin bead technology for sample preparation to allow transport for analysis at remote IAEA laboratories
- Exploration of hybrid K-edge densitometry for plutonium concentration measurements
- Implementation of Near-Real-Time Accounting for timely safeguards assessments
- Implementation of Solution Monitoring for additional assurances and C/S
- Exploration of Non-Destructive Analysis Techniques.

While these technologies were largely back-fitted to the existing facility, they formed the basis for IAEA inspections at Tokai for operations through up to the present time. With the operational history and typical throughputs experienced at Tokai, the original safeguard measures augmented by the measures implemented under TASTEX were adequate for the IAEA to make safeguards conclusions. Subsequent to commissioning of the Tokai Plant, the Japanese also built the Plutonium Coconversion Denitration Facility for conversion of Pu nitrate product from the reprocessing plant to MOX, and the Plutonium Fuels Production Facility for MOX fabrication. The IAEA gained experience with safeguards at these additional fuel cycle facilities in the mold of the TASTEX.

Through the 1980s and early 1990s, the next generation oxide reprocessing facilities emerged following both Barnwell and local national technologies. With the exception of the WAK reprocessing Plant in Germany that was subsequently cancelled before construction began, these were in Weapons states subject to Euratom safeguards (THORP, UP2-800 and UP3) and were not the subject of significant IAEA inspection responsibilities. But with the announcement of the Japanese to build the RRP, the challenge of implementation of IAEA Safeguards in the next-generation, large-scale facilities again fell to the IAEA. To advance the safeguards technology to meet the challenge, the large scale reprocessing (LASCAR) forum was convened. LASCAR was an international project between 1988 and 1992 to review effective and efficient safeguards for a large scale commercial reprocessing plant (Johnson, 1992). The USA, UK, France, Germany (FRG), Japan, IAEA and Euratom participated. They concluded that it was feasible to meet these aims using advanced techniques including NRTA.

H-2.2 Best Practice from Rokkasho-Mura Reprocessing Plant

The Safeguards Concepts and Techniques that emerged from LASCAR include four generic areas:

1. Design Information Verification – Early presentation of design information to the IAEA to allow early consultations on safeguards measures between the operator/State and the IAEA can benefit all parties. Additional benefits will accrue from continuing these consultations throughout design, construction, and commissioning.
2. Authentication of operator's instruments – It was recognized that installation of completely dedicated safeguards measurement and surveillance is preferable, particularly in the spent fuel and product storage areas, but would not likely be practical in most other areas. Use of the operator's instruments by the IAEA may be desirable and sometimes unavoidable. The simplest way for the IAEA to make use of such equipment is to take the raw (original) signal from the sensors and transmit it through tamper-resistant lines to the IAEA recording equipment.
3. Use of containment and surveillance measures – C/S measures are important, particularly in storage areas. Reliability is increased by combinations of redundant and independent techniques, such as cameras, radiation sensors, and motion detectors.
4. Data Acquisition and Transmission – This recommendation is dated with respect to modern distributed data collection systems. It recommended access by inspectors to operator accountancy systems.

The major technical findings were in the following areas:

- Submit the DIQ and initiate discussion as early as possible.
- Continue to strive to improve measurement accuracy and precision.
- Concentrate on timeliness of evaluation. Make use of C/S measures, including solution monitoring, which can be actively reviewed in a timely manner with advanced nuclear material accountancy techniques such as Near-Real-Time Accounting.
- Use C/S systems that incorporate redundant and independent features for spent fuel and product storage areas.
- Implement an on-site laboratory.
- Make use of operator measurement systems with proper authentication.

The IAEA closely and effectively followed the roadmap of the LASCAR forum. Highlights are:

- A long and regular dialog between the IAEA and the operator with the Japanese State Agency, Nuclear Material Control Center, also playing an important role.
- A comprehensive C/S and monitoring system was installed to automatically monitor receipts in the spent fuel pool in an unattended mode.
- A comprehensive C/S tracking system using cameras and radiation detectors was installed in the Head End.

The Japanese developed excellent volume measurement capabilities for the input and nitrate plutonium measurement vessels. The IAEA has also installed very accurate, independent measurement systems. The operator and the IAEA did independent analysis of calibration results. In commissioning, tests showed differences of less than 10 liters in the 20,000 liter input vessel (< 0.05%). A comprehensive C/S system for monitoring MOX product transfers to the store was installed using cameras and directional sensing radiation detectors. A solution monitoring system was installed that is significantly improved

over what was available at the Tokai Reprocessing Plant. The Japanese have developed a comprehensive NRTA system that is very non-intrusive to operations.

In cooperation with BNFL, JNFL implemented a very effective "plutonium Inventory Measurement System" to monitor and quantitatively measure material in the MOX conversion area. The IAEA is relying very heavily on the accuracy of the non-destructive measurement of inventory for the filled MOX storage cans. It is a modification of the design use at the PCDF facility. The IAEA has installed independent verification equipment for the most important measurements. They have made use of operator-installed equipment under the verification/authentication guidelines of LASCAR. An extensive on-site laboratory has been installed to allow timely analysis of IAEA samples. An effective sample monitoring system has been installed to assure proper samples are withdrawn.

H-2.3 Lessons Learned from Rokkasho-Mura Reprocessing Plant

If there are lessons learned that may be carried to a next facility, they might include:

1. There are over 70 surveillance cameras installed. Even with existing review software, the inspector time is extensive. In many of the difficult surveillance requirements, cameras were used were more creative and automated systems might have been developed.
2. Design and implementation of the software integration for the data collection and evaluation systems was started very late in the process.
3. Considerations related to proprietary information limited availability of some data that may have improved safeguards implementation and/or reduced inspection resource requirements. The IAEA has been revising its position on the shared use of operator's instruments. There can be more emphasis on developing creative authentication measures. While it was a recommendation in LASCAR to make use of operator instruments where possible, recent concerns for verification and authentication have moved the IAEA from this position.
4. A more systematic procedure for evaluation of vulnerabilities could be useful. In many cases a very ad hoc procedure was used to identify vulnerabilities and solutions were often hastily implemented without evaluations for lower cost/less inspector intensive solutions.

H-3. BEST PRACTICE – DESIGN AND CONSTRUCTION OF THE U.S. PLUTONIUM DISPOSITION MOX FACILITY AT SRS

H-3.1 Introduction

The U.S. MOX Fuel Fabrication Facility (MFFF)designed and currently being built at the Savannah River Site (SRS) for the Plutonium Disposition program is based on PUREX type processing to purify the weapons-grade plutonium, and mixed oxide fuel fabrication for use in commercial light-water reactors (LWRs), see Figures H-1 and H-2. The MFFF was designed by a consortium, originally Duke, Cogema and Stone-Webster (DCS), and based on facilities at La Hague and MELOX in France. La Hague includes two PUREX reprocessing plants (UP2-800 and UP3) located near Cherbourg, and MELOX is a MOX fuel fabrication facility located near Avignon, all having evolved through several generations of technology and design. The original industrial-scale reprocessing plant in France, UP-1 at Marcoule, commenced operation in the 1950s.

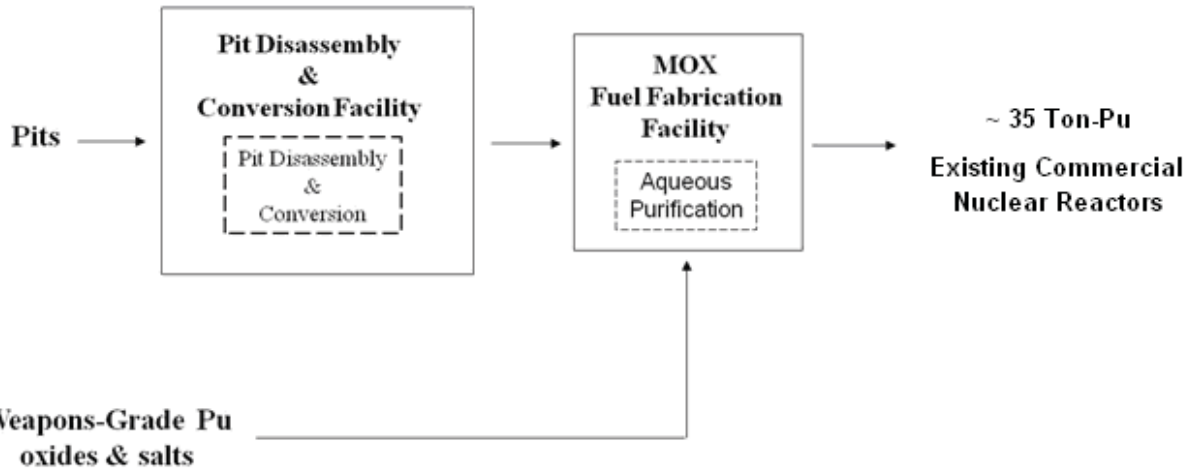


Figure H-1. U.S. plutonium disposition concept.

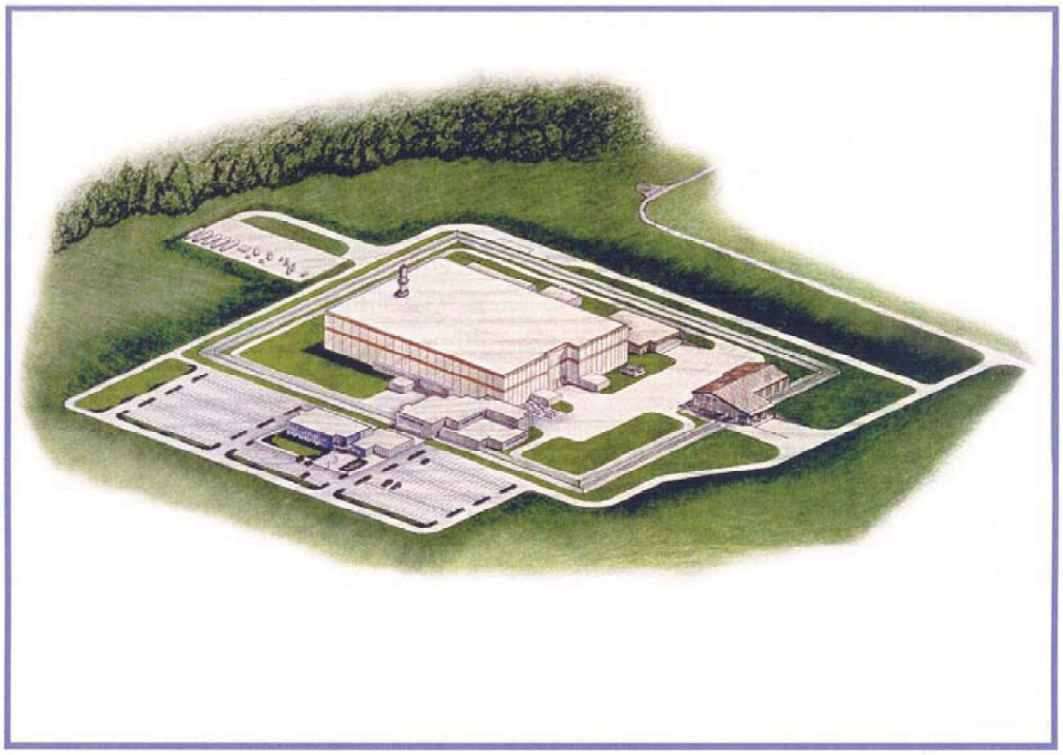


Figure H-2. U.S. MOX fuel fabrication facility (MFFF).

Before discussing issues related to "Safeguards-by-Design," it is first important to understand primary process differences between the U.S. MFFF and the French La Hague and MELOX facilities. Principal differences are (1) the use of weapons-grade rather than reactor-grade plutonium, (2) the use of PuO_2 and plutonium salts as feed rather than spent fuel, and (3) the use of existing SRS infrastructure for waste immobilization rather than integrated stand-alone operations. The use of weapons-grade plutonium requires equipment modifications due to criticality differences, which in some cases reduces throughput. The use of PuO_2 and plutonium salts as feed requires electrolytic dissolution rather than conventional nitric acid, although electrolytic dissolution had already been developed for industrial use by the French for a number of applications, one of them being waste ash dissolution for plutonium recycle. And finally, Low Level Waste will be transferred to the SRS grouting operations, High Level Waste passed on to the

Defense Waste Processing Facility, and mixed waste subcontracted to commercial entities, rather than processed by the MOX facility itself.

H-3.2 MOX Fuel Fabrication Facility Safeguards

In addition to understanding the principal process differences between the U.S. MFFF and the French La Hague and MELOX facilities, it is important to understand differences related to safeguards. The first significant safeguards difference between these facilities is the geographical separation of La Hague and MELOX. The reactor-grade PuO_2 product from La Hague is shipped hundreds of kilometers across France to MELOX, where the MOX fuel is fabricated. The U.S. MFFF consists of coupled processing and fuel fabrication operations essentially under a single roof. The other significant difference is the U.S. MFFF feedstock can be pure enough for direct weapons use, whereas the La Hague feedstock is spent fuel. MELOX feedstock is pure enough for direct weapons use, and while it is reactor-grade rather than weapons-grade plutonium, there is essentially no difference with regard to material attractiveness.

Safeguards design for the U.S. MFFF is based upon that for La Hague and MELOX, and then adapted for the U.S. NRC. La Hague and MELOX safeguards are designed to meet requirements of the French domestic regulating agency "Institute for Radiologic Protection and Nuclear Safety," which has until recently regulated both military and commercial facilities in France. In accordance with the NPT, international safeguards monitoring for La Hague and MELOX is performed by Euratom, with limited oversight by the IAEA for such things as spent fuel storage. Security design for the U.S. MFF is based on U.S. NRC and DOE requirements.

Regardless of the regulating and monitoring agency differences between France and the U.S., it is likely safeguards for La Hague and MELOX were designed in an evolutionary environment. Consequently, "Safeguards-by-Design" as defined by an early parallel design effort with process design, is not necessarily consistent with evolutionary design. The first significant safeguards design deliverable for the U.S. MFFF project was the NRC requirement for a Fundamental Nuclear Material Control Plan (FNMCP), which was not delivered until well into the overall MFFF design effort. However, because the U.S. MFFF is based on La Hague and MELOX, its safeguards design was relatively well developed early in the overall design process. In summary, while the safeguard designs for La Hague and MELOX were probably more evolutionary than "Safeguards-by-Design" oriented, and while "Safeguards-by-Design" was not a conscious approach for the U.S. MFFF, indirectly "Safeguards-by-Design" was used for the MFFF due to knowledge learned during the designs of La Hague and MELOX.

H-3.3 Best Practice – NRC Safeguards Requirements for MFFF Fundamental Nuclear Material Control Plan

Since a U.S. reprocessing plant has not been licensed by the NRC for several decades, the MFFF provided an opportunity to interpret existing NRC regulations. The process shown in Figure H-3, illustrates the high-level design methodology adopted for MFFF by DCS under NRC regulation.

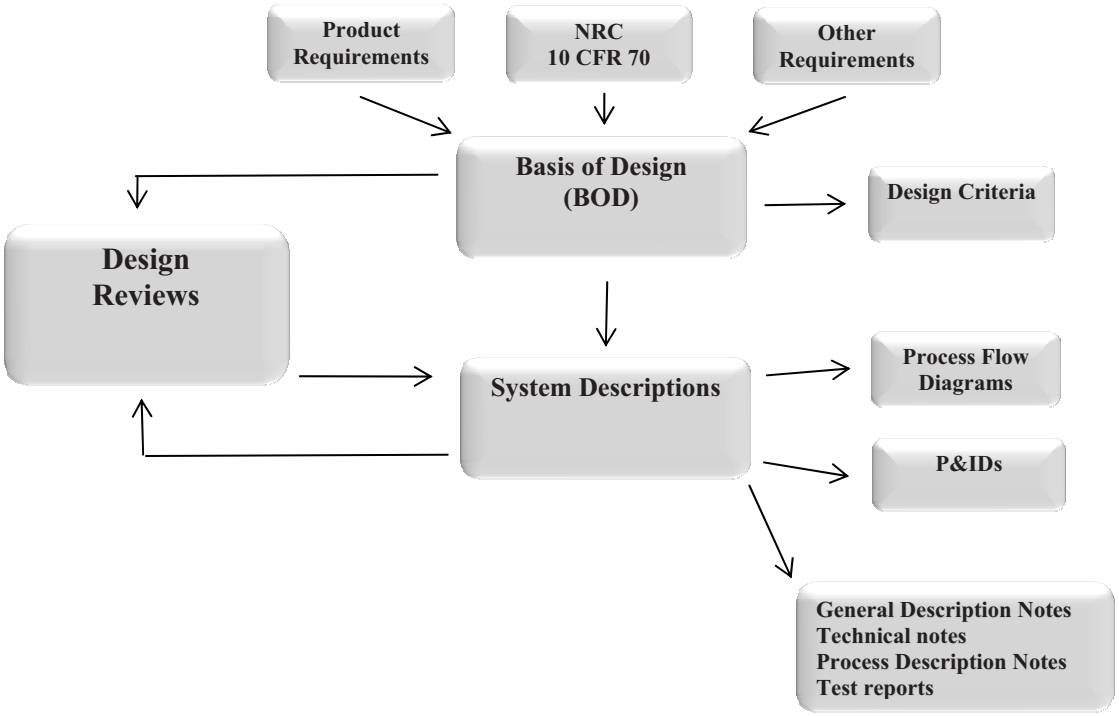


Figure H-3. MFFF design methodology in U.S.

While actual licensing has not yet been completed, significant interaction between DCS and the NRC occurred prior to issuing the FNMCP. As such, the NRC requirements identified in the FNMCP can be considered a joint interpretation by DCS and the NRC. These NRC requirements are identified at a high-level in Figure H-4 as described in the FNMCP. Two figures showing a comparison of accountancy requirements for abrupt and protracted diversion for the three agencies NRC, DOE and IAEA are given in Appendix D, Figures D-1 and D-3. These three figures reflect the requirements as described in the FNMCP.

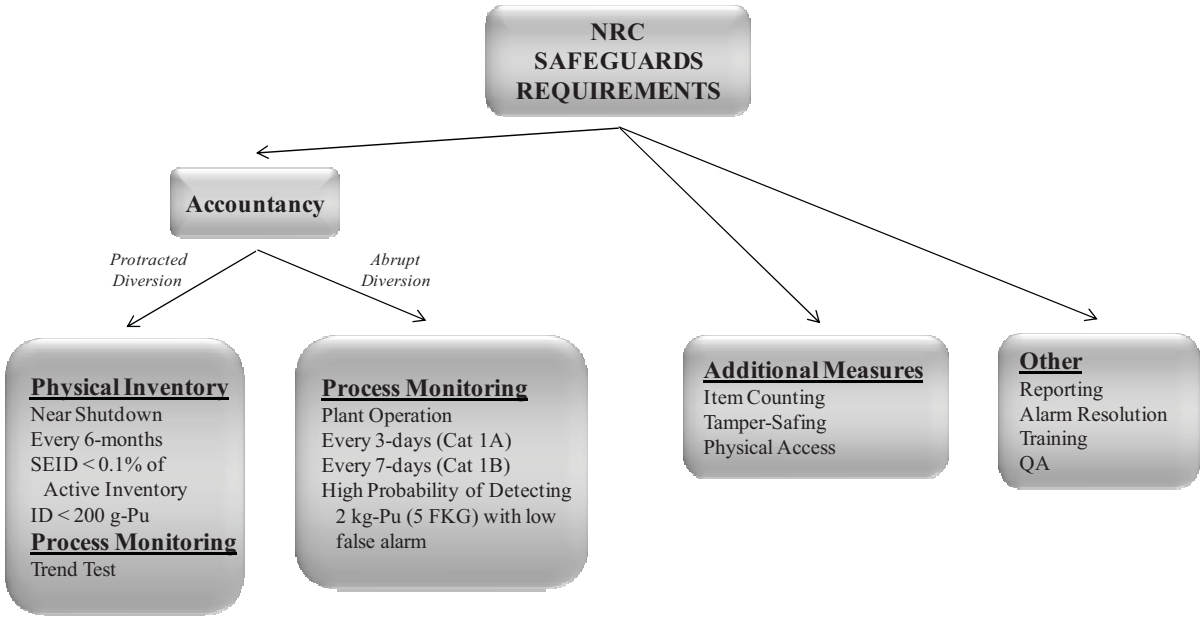


Figure H-4. NRC safeguards requirements.

H-3.4 Interpretation of the DCS Overall Design Approach for Incorporating a Parallel "Safeguards-by-Design" Effort

Since "Safeguards-by-Design" involves early participation in the overall design process, it is important to have a model of the overall design methodology. For example, it must be determined at what extent of the process design the safeguards instrumentation for protracted diversion accountancy should be incorporated. A similar, but more specific development of the safeguards design methodology can be superimposed on the overall design methodology, in order to place the safeguards design effort in phase with the overall design effort. This activity can form the basis for defining early safeguards deliverables, which can then become specified in the regulating/monitoring agencies (DOE, NRC and IAEA) requirements.

The MFFF experience in the U.S. can provide an example of the overall design methodology for a reprocessing and fuel fabrication nuclear facilities. Figure H-3 represents a top-level view of the design process used for the MFFF. The details of Figure H-3 are what need to be synchronized with the safeguards design activities.

H-3.5 Additional Points

For the MFFF, additional points may enter the realm of DCS proprietary information and will be left to future efforts that avoid this conflict.

H-4. BEST PRACTICES – DEVELOPMENT OF UNCLASSIFIED SAFEGUARDS REQUIREMENTS DOCUMENTS

One of the challenges to the implementation of Safeguards-by-Design within the Department of Energy is that much information related to safeguards requirements and measures is contained in classified documents, such as the vulnerability analysis. Since the issuance of security clearances is strictly limited to those individuals needing routine access to classified information, it is quite likely that most members of a facility design team will not have the requisite clearances to access these classified documents. This compartmentalization of information, though necessary for national security, has the potential to seriously hinder the integration of safeguards into design. The various security program representatives may be uncertain about the level of detail that they can provide to designers, who do not possess security classification. Their discussion of security measures with designers may be limited to giving the designer specific instructions about interfaces without being able to say why specific things need to be done. This lack of information may make it difficult for the designer to identify opportunities to make design modifications that would reduce cost and better integrate the safeguards measures into the overall design. The compartmentalization of information also makes it difficult for designers to understand those design changes that might affect security so that security program representatives can be consulted about the potential impacts. It is also possible that a subtle safeguards requirement in a classified document may not be provided to the designers until the security program representatives review and comment on a proposed design, making the safeguards requirement one of the last considered. Finally, classification requirements make it more expensive and difficult to employ computer-based system engineering tools since these tools must be used in a classified computing environment. As a result, the safeguards requirements are frequently tracked separately and are not necessarily integrated effectively into the overall design.

Recognizing these potential problems, one Department of Energy project, which is in the preliminary design stage, is developing an unclassified safeguards requirements document for the project based upon the vulnerability assessment and the DOE directive requirements for safeguards and security. This safeguards design requirements document is intended to be analogous to Chapter 4 of the Preliminary Documented Safety Analysis, which identifies the safety systems and measures and their performance

requirements without addressing the accident scenarios that drive the selection of systems and performance requirements. The hope is that such a document can be developed in a manner that is comprehensive and reasonably informative to the designers, but that requires protection at no higher level than Unclassified Controlled Nuclear Information (UCNI). Such a document can be shared with the designers on a need-to-know basis once they have been trained regarding the control and protection of UCNI. Since aspects of these designs other than the security measures are UCNI, the design project would, in any case, need to be equipped to store, handle and protect UCNI and to do UCNI data processing. Therefore, this does not create any unique cost or administrative burden beyond the development of the UCNI safeguard requirements document.

This approach, if initiated during the initial vulnerability assessment during conceptual design, has the potential to enhance Safeguards-by-Design throughout the design and construction process. It can ensure that the designers in all disciplines are more aware of safeguard requirements – both the performance driven ones from the vulnerability assessment and the compliance driven ones from DOE directives. This will allow the designers to better understand where design changes might affect security performance and to identify areas where security features can be effectively integrated with other design features. This approach will also provide a set of security requirements that can be treated on a comparable with other requirements using systems engineering tools and techniques. Similarly the requirements document will permit expeditious evaluation of field changes during construction to ensure that they do not degrade safeguards.

The DOE project discussed is just beginning to implement this approach and its overall effectiveness remains to be seen. The Implementation of Safeguards-by-Design (ISBD) project will continue to monitor the effectiveness of the design and construction project's efforts in this area and will incorporate proven aspects into the more detailed proposed guidance for ISBD.

H-5. BEST PRACTICES – EVOLUTION OF INTEGRATION OF SAFEGUARDS

H-5.1 Introduction

Safeguards and security comprise or are affected by many inter-related aspects or parts. There are many 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. This section is a brief review of best practices drawn over the period of the last three decades. Various models for integration are identified, driving forces summarized and outcomes described. DOE and NRC approaches are outlined. Since around the year 2,000, the term "integrated safeguards" has taken a new 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 CSA and the AP. This arose from perceived deficiencies in the previous approach relying mainly on the CSA.

Safeguards 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 context "integrated" means "made up of aspects or parts that work well together." So in this report "integration of safeguards" means "the activity of fitting together appropriate aspects or parts of safeguards that work well together and form an optimized system." A potential endpoint is the unification of all safeguards activities into a single system but, a priori, this is not necessarily the optimum.

H-5.2 Integration Approaches

Early work includes four papers, which were presented to the 17th Annual INMM Meeting in 1976 (Carlson 1989). Historically, it has been common to divide safeguard activities into two wide categories: security (physical protection) and material control and accounting (MC&A), which have been regulated or licensed as separate entities by DOE and NRC respectively. Recently, these two categories have been extended somewhat in the U.S. by definition as PP (physical protection) robustness and PR (proliferation resistance); the former relating to threats from sub-nationals and the latter from owner nation-states (Evaluation of methodology for PR and PP of Gen IV Nuclear Energy Systems, GIF/PRPPWG/2006/005). This appendix is a preliminary examination of integration of safeguards and a more comprehensive study is recommended for FY 2009.

Alternative high-level integrated safeguards concepts have included (Carlson, 1989) 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. Analogously, the use of a single 10 CFR Part has been proposed for commercial licensees. This was proposed to reduce regulatory inconsistencies and potential conflicts and to streamline compliance by the licensee. None of these steps has been taken to date. Safeguards definitions in U.S. Department of Defense, U.S. DOE and U.S. NRC and others are not always consistent. For example, without a clear definition of integrated safeguards, the objective and means of its attainment may become unclear. GAO drew attention to lack of overall strategy that integrates the threat reduction and nonproliferation programs of these organizations (GAO-05-157, January 2005).

Early alternatives to integration of the two classes; security and MC&A (now commonly described as PP and PR) covered integration (3 part) via personnel control, material operations, and control and material accountability. Other suggested integration of MC&A with facility process control and another added information, safety and planning. These were generally associated with commercial reprocessing plants designed but not built and/or operated and the proposed approaches were not deployed.

A major opportunity lay in integration of data (Carlson, 1989) stemming from security, material control, material accountability, process control and quality control. Like safety, the philosophy for safeguards data has been to generate, transmit and present this separately from facility process control and other functions. The initial emphasis was placed on integration of material control and process control; in fact the former is a specific example of the latter and so there is a natural fit. Further integration of security, accountability and quality control was recommended and considered straightforward. It is considered that this overall opportunity has been successfully exploited, now considered commonplace and largely stemmed from the rapid, wide deployment of personal computer, dedicated control stations and information technology more generally, since that time. However, independence of some safeguards and safety instrumentation, signal transfer and data processing is often still a requirement to preserve integrity. The example of the Hanford Fuels and Materials Examination Facility design was quoted as a best practice of the era.

H-5.3 U.S. DOE Practice

The DOE National Nuclear Security Administration (NNSA) is responsible for the management and security of the nation's nuclear weapons, nuclear nonproliferation, and naval reactor programs. It provides safe and secure transportation of nuclear weapons and components and SNM along with other missions supporting the national security. The responsibilities of the DOE Office of Health, Safety and Security include safety analysis; corporate safety and security programs; and complex-wide independent oversight; and enforcement. The DOE Office of Nuclear Energy has responsibilities for protecting assets at INL using Protective Forces, Security Systems, Transportation, Information Security, Personnel Security, Material Control and Accountability, Program Management and Cyber Security. DOE integrates these

responsibilities and many others by various means. Within the DOE, directives are the primary means for one office to promulgate long term direction affecting other parts of the Department.

In line with the conventional separation of physical security and safeguards, the manual, DOE M 470.4-2 Chg 1, Physical Protection, establishes requirements for the physical protection of safeguards and security interests while DOE M 470.4.3 Chg 1, Protective Force, establishes requirements for management and operation of the DOE Protective Force, including firearms operations and training. Under the safeguards area, DOE M 470.4-6 Chg 1, Nuclear Material Control and Accountability, establishes a program for the control and accountability of nuclear materials within the Department. The guide, DOE G 413.3-3, Safeguards and Security for Program and Project Management , Section III, reviews the program background and integrates safeguards and security including reference to the DOE O 470 series of directives (all issued by Office of Health, Safety and Security - HS), which establish minimum design principles. A specific area where there is evidence of integration between physical protection and material control is in Chapter III of Section A, Materials Control, of DOE M 470.4-6 Chg 1. Additionally, DOE O 413.3A, Program and Project Management for the Acquisition of Capital Assets Issued by Office of Management – MA), p.32-33 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 order DOE O 470.4A, Safeguards and Security Program requires that programs be developed and that directives are implemented as shown in Table H-1.

Table H-1. Required Directives from DOE O 470.4A, Safeguards and Security Program.

No.	Subject
DOE O 226.1	Implementation of DOE Oversight Policy, 9-15-05 (HS)
DOE P 470.1	Integrated Safeguards & Security Management (ISSM) Policy, 5-08-01
DOE M 470.4-1 Chg 1	Safeguards and Security Program Planning and Management, 8-26-05
DOE M 470.4-2 Chg 1	Physical Protection, dated 8-26-05
DOE M 470.4-3 Chg 1	Protective Force, dated 8-26-05
DOE M 470.4-4	Information Security, dated 8-26-05
DOE M 470.4-5	Personnel Security, dated 8-26-05
DOE M 470.4-6 Chg 1	Nuclear Material Control and Accountability, dated 8-26-05
DOE M 470.4-7	Safeguards and Security Program References, dated 8-26-05

Some other important directives relating to safeguards and security and their integration within DOE including their realization through programs and projects are shown in Table H-2.

Table H-2. Directives relating to DOE O 470.4A, Safeguards and Security Program.

No.	Subject
DOE O 142.2A	Voluntary Offer Safeguards Agreement and Additional Protocol with the IAEA – National Nuclear Security Administration (NA)
DOE P 205.1	Departmental Cyber Security Management Policy – Information Management (IM). Others include: DOE O 205.1A (IM), DOE M 205.1-3 (IM), DOE M 205.1-4 (IM)
DOE G 226.1-1	Safeguards & Security Oversight & Assessments Implementation Guide (HS)
DOE P 410.1A	Promulgating Nuclear Safety Requirements (HS/GC, Office General Counsel)
DOE P 413.1	Program and Project Management Policy for the Planning, Programming, Budgeting, and Acquisition of Capital Assets (MA). Others include: O 413.3A (MA), M 413.3-1 (MA), G 413.3-3 (HS)
DOE O 420.1B	Facility Safety (HS). Others include: DOE G 420.1-1, DOE G 420.1-2, DOE G 420.1-3 (HS)
DOE O 461.1A	Packaging and Transfer or Transportation of Materials of National Security Interest (NA)
DOE P 470.1	Integrated Safeguards and Security Management (ISSM) Policy (HS). Others include: DOE O 470.2B, O 470.3A, O 470.4A (all HS)
DOE O 5560.1B	Management of Nuclear Materials (NA)

In summary, DOE integrates the safeguards and security system through a broad range of directives from various Offices. The objective identified above by Carlson, 1989, of the integration of these as a single directive, i.e., single document, from a single Office may be inappropriate and the modular approach, as used, more practicable unless use of a simple performance-based approach is adopted.

H-5.4 U.S. NRC Practice

Concerning regulation of commercial facilities by NRC, the relevant Codes of Federal Regulations, shown in Table H-3, include:

Table H-3. Federal Regulations Codes.

No.	Subject
10 CFR Part 11	Criteria & Procedures for Determining Eligibility for Access to or Control over Special Nuclear Material
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

It can be seen that Physical Protection is dealt with in a separate code to material control and accountability 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 along the lines identified above (Carlson, 1989). The recent NRC Draft Regulatory Guide DG-5021, July 2007, Managing the Safety/Security Interface, provides the proposed addition of Section 73.58 to 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 draft guide may provide a useful model relating to physical security and safeguards aspects.

H-5.5 IAEA Integrated Safeguards

Regarding international safeguards, the detection of undeclared nuclear materials and activities is considered the greatest contemporary challenge. The IAEA expresses this as the need for international safeguards to provide assurance of the completeness of a State's declaration as well as its correctness for the activities declared. Here the IAEA is meeting the definition that "integration of safeguards" means "the activity of fitting together appropriate aspects or parts of safeguards that work well together and form an optimized system." 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, which are incredible in the national safeguards context.

H-6. LESSON LEARNED - THORP PROLONGED HIGH ACTIVE LIQUOR LEAKAGE TO CELL

H-6.1 Introduction

On 20 April 2005, British Nuclear Group Sellafield Limited (BNGSL), formerly British Nuclear Fuels Limited (BNFL), discovered a leak from a pipe that supplied highly radioactive liquor to an accountancy tank in a part of the Thermal Oxide Reprocessing Plant (THORP) at Sellafield, known as the 'feed clarification cell' (HSE, 2007). Approximately 83 m^3 of dissolver product liquor, containing ~ 22 tons of spent nuclear fuel [including ~ 160 kg(Pu)], had leaked onto the floor of the cell. The leak began prior to 28 August 2004 and remained undiscovered until 20 April 2005. The leak was relatively small until January 2005 when complete failure of the nozzle is believed to have occurred. Video evidence indicated that the leak came from a pipe, identified as nozzle N5, which had completely severed just above where it enters accountancy tank B (HEAT B - Head End accountancy tank). The most likely cause was fatigue failure from the swinging/swaying motion of the suspended tank, which occurred during agitation of the tank contents as part of normal operation. The motion occurred because of inconsistencies in the later stages of design and during construction, together with a modification to the operational mode of the vessel ca. 1997, which inadequately considered the impact on pipe-work. These failures were not identified due to inadequate monitoring arrangements and management oversight. All indications are that the leaked liquor was contained in the cell and it is accepted that there was no possibility of a criticality from the incident. The leaked liquor was successfully returned to primary containment.

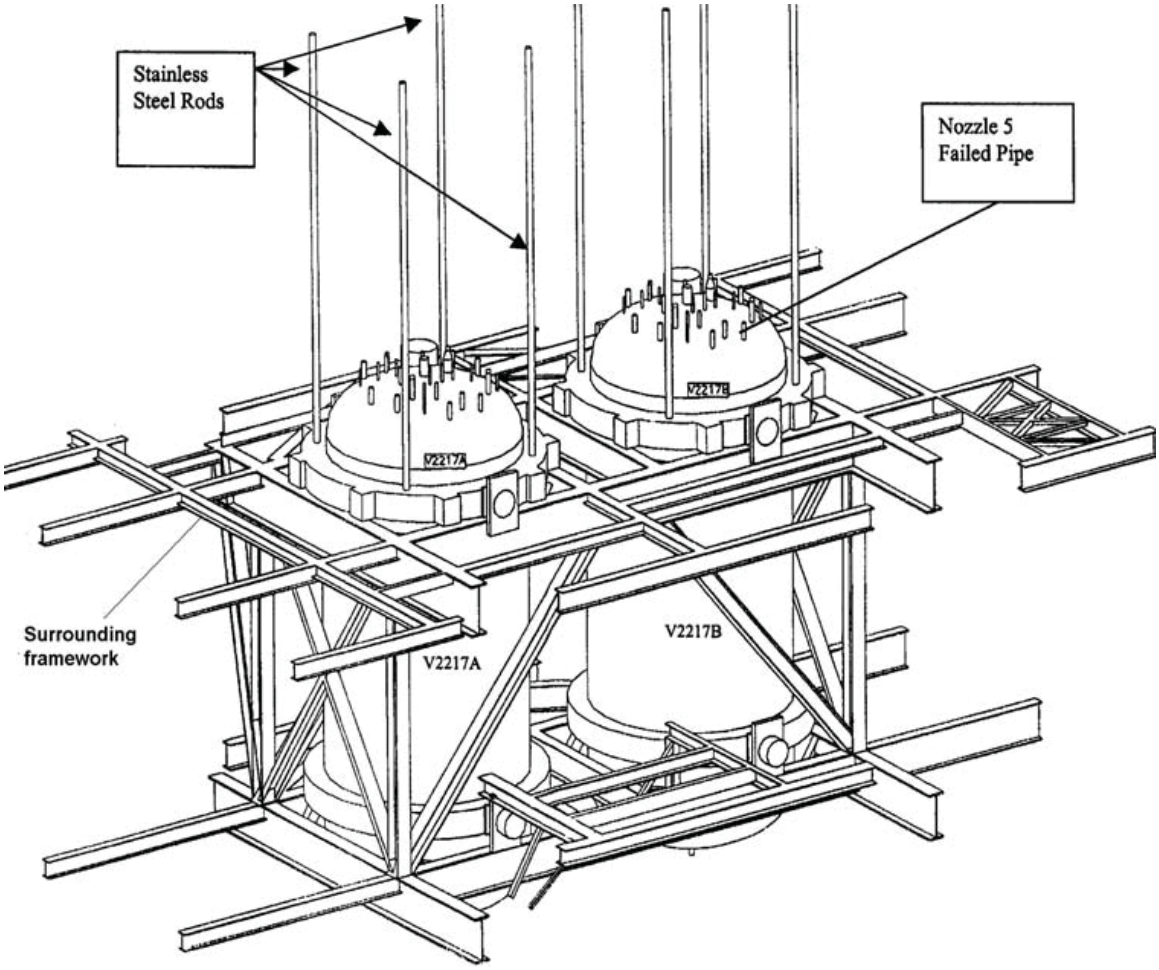


Figure H-5. Line drawing of accountancy tanks V2217A and V2217B, hanger rods and surrounding framework.

The UK Health and Safety Executive (HSE), Her Majesty's Nuclear Installations Inspectorate conducted an investigation and found BNGSL had been in breach of nuclear site license conditions at the Sellafield Site (Ref. 1). Three of these breaches were serious, continued over a prolonged period of time and directly contributed to the incident. BNGSL pleaded guilty to these offences in Court. The company was fined a total of $0.75M (£0.5M) with costs of $100k (£67,959). THORP was shut down following the incident and required a formal consent from HSE before being allowed to begin reprocessing operations again. Consent was granted on 9 January 2007. Shearing of spent fuel re-started on July 4, 2007 and was processed by solvent extraction in November 2007, 30 months after the forced shutdown. This severely affected BNGSL reprocessing performance for utility customers. The lessons learned are considered to be surprisingly wide ranging and have significance far beyond the immediate damage done or need for equipment repairs.

H-6.2 Observations and Corresponding Lesson Learned

Safeguards Modeling Observations:

- Failure to account for up to 20 IAEA significant quantities (ca. 160 kg total) of plutonium for up to 8 months, which is in direct contradiction to corporate safeguards requirements and expectations. IAEA requires detection of one significant quantity unaccounted within 1 month.

- Known area of statistical weakness at front-end of PUREX process – good precision, i.e., < 1% error in analyses, only starts at first accountancy tank – liquor measurement of homogeneous bulk of material.
- Apparent low expectation by staff of precision of data from utilities. High shipper receiver differences tolerated.

Lesson Learned 1 – The current safeguards system should be improved for earlier detection and reporting of loss of material control for much lower levels of nuclear material unaccounted for.

Engineering Observations:

- Inconsistencies and lack of configuration control during design and engineering of THORP accountancy tanks. Modifications poorly carried out without understanding of safety significance. Modified the operational mode of the vessel without adequate consideration of impact on pipe-work.
- Dark cell – sealed cell design approach – no routine periodic TV/camera scans for re-assurance of no unexpected gross conditions. HA liquor movements have to stop when cameras placed in cell – not facile operation.
- It was not the installed leak detection systems that led to the discovery of the leak. It was the analysis of nuclear materials accountancy discrepancies of several fuel shearing campaigns that led to the detailed investigations on the plant, and subsequently to discovery of the leak.

Lesson Learned 2 & 3 – The control of design, engineering and plant operations should be improved especially in areas with significant safeguards and safety impact. The cost and benefits of improved inspection of plant condition should be examined and programs implemented as necessary.

Operational Culture Observations:

- "Invincible plant" so failures of plant integrity not expected.
- Plant production below design targets – culture of keep operating whenever possible despite some equipment response abnormalities.
- Ignoring of alarms, non-compliance with operating instructions, safety-related equipment not in effective working order, and absence of questioning attitude. This culture and approach became the norm.
- Operational culture – bubbler leak detectors in cells not maintained properly and not operational to detect leakage.

Lesson Learned 4 – A step change in the management/staff culture of tolerating operational deficiencies should be made to raise the standard of safeguards and safety performance.

Management Effectiveness Observations:

- Weaknesses in roles and responsibilities and lack of effectiveness of monitoring, audit and review. Failure to learn from previous events and lack of embedding of early lessons learned.
- Contravened legal regulations including: safely operating sumps according to written instructions, operated plant without adequately working pneumercators, and operated a leaking HA pipe work system for 9 months without detection.
- Adoption of IAEA guidance on questioning attitude and culture of challenging and accepting challenge is needed – Management and workforce.
- The HSE said there was no evidence of harm to workers or the public but said it was "not prepared to tolerate" a "significant prolonged reduction in attention – the plant must also be operated, maintained and managed to high standards we insist on."

Lesson Learned 5 – A marked improvement in the culture of accountability, receptiveness to lessons learned and attention to unexpected or unusual plants conditions should be instigated.

Financial Impact Observations:

- Loss of 2.5 years reprocessing throughput, nominally 1,750 ton, has had a severe effect on the finances of the UK Nuclear Decommissioning Authority, who are the owners of THORP.

Lesson Learned 6 – Higher facility operational standards and culture should be made to support sustained plant operation and financial viability dependent on the retention of regulatory and other stakeholder confidence.

Organizational Change Observations:

- Previous operational, environmental, financial and legal infringements over several decades causing fundamental organizational review by UK Government. This incident confirmed their drastic intent.
- BNGSL and its parent BNFL, state-owned companies, have been broken up and privatized. A five-year contract to manage the Sellafield complex including D&D was awarded to the international, private-sector consortium of URS (Washington Division), AREVA and Amec in 2008 following the U.S. Management and Operations model.

Lesson Learned 7 – Improvement of site operational standards and culture should be made for successful retention of Management and Operations contract.

H-6.3 Summary of THORP Lesson Learned

This is as follows:

1. The current safeguards system should be improved to provide earlier detection and reporting of loss of material control at much lower levels of nuclear material unaccounted for.
2. The control of design, engineering and plant operations should be improved especially in areas with significant safeguards and safety impact.
3. The cost and benefits of improved monitoring and inspection of plant condition, particularly with regard to grading and increased frequency, should be examined and programs implemented as necessary.
4. A step change in the management/staff culture of tolerating operational deficiencies should be made to raise the standard of safeguards and safety performance.
5. A marked improvement in the culture of accountability, receptiveness to lessons learned and attention to unexpected or unusual plants conditions should be instigated.
6. Facility operational standards and culture should be raised to support sustained plant operation and financial viability dependent on the retention of regulatory and other stakeholder confidence.
7. Improvement of site operational standards and culture should be made for successful retention of Management and Operations contract.

H-7. CONCLUSIONS OF APPLYING BEST PRACTICES AND LESSON LEARNED TO ISBD

The principal conclusions from these examples of best practice and lessons learned are as follows:

- Next Generation Facilities - Safeguards-by-Design (SBD) has the potential to give greatest benefit where facility design is being conducted using a "clean-sheet" approach and alternatives selection, for example: flowsheet, equipment selection and layout, is less constrained by existing practice. Next generation plants are also more likely to be given more radical or "step-change" design requirements calling for innovative concepts and are more likely to be accommodating of intrinsic design improvements.
- Mixed Oxide Fuel Fabrication Facility - The La Hague reprocessing and MELOX fuel fabrication plants were designed and developed, including safeguards aspects, over several generations of facilities in an evolutionary environment spanning about five decades. SBD as defined by an early safeguards design effort in parallel with process, equipment and facility design, may have less beneficial impact where overall design is largely unchanged from one facility to the next, although regulatory differences usually exist between different countries. Whilst safeguard designs for the French facilities were probably more evolutionary than SBD oriented, design integration and SBD took part in MFFF design due to knowledge learned during La Hague and MELOX design.
- Rokkasho-Mura Reprocessing Plant - The IAEA safeguards system for RRP represents a world best practice as developed from long plant experience, several international development reviews and an earlier major pilot reprocessing facility in Japan. IAEA safeguards at RRP are deemed to be effective, but possibly not as cost effective as would have been the case where safeguards were fully integrated into design from the pre-conceptual planning stage. Like MFFF, RRP was designed using French technology and know-how, and so benefitted from knowledge learned during design and operation of UP-2/UP-3.
- Safeguards Integration – The focus of integration of safeguards changes with time depending on contemporary challenges and a wide range of approaches have been proposed over the past several decades. Safeguards and security comprise or are affected by so many inter-related aspects or parts that integration to a single entity appears impractical and priorities and best-fit must govern. As an example, success in integration of data needs has been successful to the point of being considered routine whilst other proposals, such as integrating physical protection with material transfer, are not accepted.
- Sellafield Thermal Oxide Reprocessing Plant – The prolonged HA leakage to a process cell showed weaknesses in the design process, facility design, inadequate plant monitoring and operation, operational and management cultures, safeguards modeling, and safety culture. Whilst SBD is a valuable integrating technique (and might possibly have helped avoid the initiating failure), this incident demonstrates the importance of wider integration across the whole facility lifecycle including design (part of which is RAMI = reliability, availability, maintainability, and inspectability), commissioning, operations, and safeguards activities (especially MC&A and modeling). A severe breach of corporate safeguards requirements and expectations occurred showing a serious lack of integration with plant operations and maintenance.

Appendix I

Guiding Principles for Safety-in-Design

Appendix I
Guiding Principles for Safety-in-Design

The following excerpt from DOE-STD-1189-2008, "Integration of Safety into the Design Process," is a useful partial template of best practices in the design process. Many of these principles are directly applicable to Safeguards-by-Design.

SAFETY DESIGN GUIDING PRINCIPLES

1. DOE Order 420.1B, Facility Safety, is utilized and addressed in design activities, as applicable. Design teams should be able to clearly articulate strategies in the design that address DOE O 420.1B expectations and include them in the design/safety basis information.
2. Control selection strategy to address hazardous material release events is based on the following order of preference at all stages of design development.
   - Minimization of hazardous materials is the first priority.
   - Safety structures, systems, and components (SSCs) are preferred over Administrative Controls.
   - Passive SSCs are preferred over active SSCs.
   - Preventative controls are preferred over mitigative controls.
   - Facility safety SSCs are preferred over personal protective equipment.
   - Controls closest to the hazard may provide protection to the largest population of potential receptors, including workers and the public.
3. Controls that are effective for multiple hazards can be resource-effective.
4. Design codes and standards incorporated into the DOE O 420.1B guides are to be followed, unless specific exceptions are taken to those listed and approved by DOE.
5. The risk and opportunity assessment includes consideration of the Safety-in-Design approaches selected to address project cost contingencies and appropriate mitigation strategies for the risks/opportunities identified for the strategies selected.
6. Early project decisions on a technical approach are conservative in order to establish appropriate cost and schedule baselines for the project.
7. The Critical Decision (CD) packages portray safety-item selections, bases, and risks and opportunities, with proposed mitigation strategies and cost and contingencies, to enable informed risk decision-making by the project approval authorities regarding the project technical basis and cost.
8. The project team includes appropriate expertise and is established early in the project cycle.
9. Safety personnel are used from the onset of project planning to help ensure that appropriate hazards and techniques for hazard management are considered (e.g., material-at-risk [MAR] limitation, prevention techniques, and operationally effective design solutions).
10. Important safety functions, such as facility building confinement, confinement ventilation approach and systems, fire protection strategies and systems, security requirements, life safety considerations, emergency power systems, and associated seismic design bases are addressed during conceptual design.
11. The safety design team ensures sufficient process definition is available, particularly at the conceptual and preliminary design stages, to enable major safety cost drivers to be included in the design documentation, along with their associated safety functions and design criteria. The team also identifies the risks and opportunities associated with the selections identified and develops mitigation

strategies that are included in the cost-estimate contingencies. Details may not be available in early project stages to identify all hazards and needed hazard controls.

12. All stakeholders are important to the process. Stakeholder issues are identified early and addressed.
13. To ensure that the project/facility configuration can be managed appropriately, the basis for decisions related to safety is clearly documented.

Appendix J

Outline for Possible DOE Directive on Safeguards-by-Design

Appendix J
Outline for Possible DOE Directive on Safeguards-by-Design

The following is the description of a potential future ISBD deliverable:

OUTLINE FOR POSSIBLE DIRECTIVE ON SAFEGUARDS-BY-DESIGN

Appendix K

Survey of NRC Arena for Application of Safeguards-by-Design

Appendix K
Survey of NRC Arena for Application of Safeguards-by-Design Process

K-1. NRC'S REGULATORY PROCESS FOR COMMERCIAL NUCLEAR POWER FACILITIES

The U.S. Nuclear Regulatory Commission (NRC) regulates the construction and operation of new commercial nuclear power facilities. The NRC is responsible for issuing standard design certifications, early site permits, construction permits, operating licenses, and combined licenses for commercial nuclear power facilities. NRC regulates reactor siting, construction, and operation through a combination of regulatory requirements, licensing, and oversight, including inspection. The current regulatory infrastructure is generally adequate to support new licensing. NRC issued Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants," for public use in June 2007. This regulatory guide reflects major revisions to 10 CFR Part 52 (Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants) and NUREG-0800 (Standard Review Plan) that were issued in early 2007. A combined license (COL), when issued, is authorization from the NRC to construct and, with conditions, operate a nuclear power plant at a specific site and in accordance with laws and regulations. NRC staff issued NRO-REG-100, Draft Revision 1, "Acceptance Review Process for Design Certification and Combined License Applications," dated January 7, 2008, for use and comment. COL applications for around 15 new reactor units have already been received and more than 20 are expected. NRC commenced establishing the new COL application process in 1989 and this was refined and updated with a rule-making in 2007. NRC also issued recently a NUREG document, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing," NUREG-1860, December 2007, which gives a "Framework" that provides an approach, scope and criteria that could be used to develop a set of requirements that would serve as an alternative to 10 CFR 50 for licensing future NPPs. This Framework is not the entire process but rather a significant piece of research.

The FY-08 ISBD Project brief was focused on improvement of Safeguards for capital acquisitions within the DOE complex. In this appendix, information gathering was performed and the status reported to identify differences with the commercial, NRC regulated arena. Potential future approaches for introduction of the SBD process within NRC fuel licensing of fuel facilities are also proposed.

K-2. NRC'S REGULATORY PROCESS FOR NON-REACTOR FACILITIES

The following is a brief description of the NRC regulations related to the licensing of various commercial non-reactor nuclear facilities.

Part 10 CFR 70, Domestic Licensing of Special Nuclear Materials, is the regulation governing the design, construction, and operation of most NRC non-reactor nuclear facilities. Some of the requirements of this regulation are as follows:

- 10 CFR 70.62 requires an ISA for facilities that contain quantities greater than a critical mass of SNM to include scenarios, likelihoods, radiological hazards, chemical hazards.
- A Decommissioning Plan must be developed with funding.

- If an enrichment facility, an M&C plan must be developed in accordance with 10 CFR 74.
- Each application for a license to possess and use SNM in a plutonium processing and fuel fabrication plant shall contain, in addition to the other information required by this section, a description of the plant site, a description and safety assessment of the design bases of the principal structure, systems, and components of the plant, including provisions for protection against natural phenomena, and a description of the quality assurance program to be applied to the design, fabrication, construction, testing and operation of the structures, systems, and components of the plant.
- Facilities must have a physical protection plan, including transport if licensed to do so, in accordance with 10 CFR 73.
- If specific quantities of attractive SNM are planned, facilities must include a licensee safeguards contingency plan for dealing with threats, thefts, and radiological sabotage.
- An emergency response plan must be developed if offsite dose requirements cannot be met. To include training, notification and co-ordination, exercises.
- A criticality safety program must be developed.
- A fire protection and explosion mitigation program must be developed.
- In response to a written request by the Commission, an applicant for a license to possess and use more than one effective kilogram of SNM shall file with the Commission the installation information described in § 75.11 of this chapter on Form N-71. The applicant shall also permit verification of such installation information by the IAEA and take such other action as may be necessary to implement the US/IAEA Safeguards Agreement, in the manner set forth in § 75.6 and §§ 75.11 through 75.14 of this chapter.

However, under current regulations, a new commercial reprocessing facility, using for example advanced PUREX or UREX+ flow sheets, would be defined as a “production facility” under the Atomic Energy Act of 1954, as amended, and would presently require a license under the regulations in 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities.” In contrast, plutonium processing and fuel fabrication facilities are licensed in accordance with the regulations in 10 CFR Part 70, “Domestic Licensing of Special Nuclear Material.” Licensing a new commercial reprocessing facility would present a challenge because it would be the first production facility licensed in the past 40 years, and the facility's operational characteristics would differ significantly from the LWRs that are typically licensed under Part 50 (NRC, SECY-06-0066, 2006)

A production facility is defined in 10 CFR 50.2 generally as (1) any nuclear reactor designed or used primarily for the formation of plutonium or uranium-233; (2) any facility designed or used for the separation of the isotopes of plutonium; or (3) any facility designed or used for the processing of irradiated materials containing SNM, with the exception of facilities that handle small quantities of SNM and some facilities in which processing is conducted pursuant to a license issued under parts 30 and 70.

K-3. NRC’S LICENSING OF ADVANCED RECYCLING FACILITIES

A key feature of recent GNEP deployment studies, as performed by several international industrial consortia on behalf of DOE, is the proposal to re-establish advanced nuclear fuel recycling in the U.S. Such processing may establish new products, such as plutonium mixed with minor actinide(s), and extended partitioning of wastes. As discussed by NRC (NRC, SECY-06-0066, 2006), a reprocessing facility uses processes similar to those used in a MOX facility, which would be licensed under the Part 70 licensing process. In addition, Part 50 is focused on LWR design and technology and would have limited applicability to commercial reprocessing facility design and technology. The design and operational safety issues associated with a commercial reprocessing facility would be very different from design and operational safety issues associated with an LWR. The current Part 50 regulations would not necessarily

address all commercial reprocessing facility safety issues and, conversely, are likely to contain requirements that are not applicable to a reprocessing facility. The application of the whole of Part 50 to the licensing of a commercial reprocessing facility would present significant challenges to the applicant and to the NRC. If Part 50 is used to license a commercial reprocessing facility, the regulations would have to be reviewed to determine which apply, do not apply or may partially apply. Additional requirements would also need to be established to address reprocessing facility-specific design and safety issues. Once applicability determinations are made, a possible approach to establish a licensing framework would be to use a process similar to that used for centrifuge enrichment facility licensing (Louisiana Energy Services, National Enrichment Facility).

At a low level of resources, NRC is preparing for licensing potential nuclear fuel recycling in the U.S. after an interval of about three decades. Through an interagency NRC-DOE MOU agreement on GNEP, DOE is funding a modest level of study associated with international operational reprocessing technologies. NRC will provide regulatory insights based on information provided by DOE, et al.; NRC is undertaking a gap analysis on current NRC regulations and technical bases documents. Incorporating the results of the gap analysis into the existing regulatory structure, either by amending current regulations or creating a new regulatory structure for recycling would involve multiple, simultaneous rulemakings and parallel development of the associated regulatory guidance documents. Such rulemakings would, to the extent practical, be risk-informed and performance-based and would be written to address the safety, technical and policy issues which are specific to reprocessing facilities. The current Part 70 would provide a good framework for such revisions or a new rulemaking. Additional staff resources would focus on the development of appropriate regulatory guidance. NUREG-1718, “Standard Review Plan for the Review of an Application for a Mixed Oxide Fuel Fabrication Facility,” would be a good basis for the development of guidance for the review of a reprocessing facility.

This process would take at least two years to complete and another one to two years to issue the final rule, and would require several full-time employees. The resource estimate increases to $10 million per year if a new regulation is developed, extensive public outreach is conducted, and a programmatic environmental impact statement is developed. NRC needs a better understanding of industry’s intentions before committing such expenditure and suggests that industry form technical working groups, where the example of Part 52 rulemaking provides examples of where this approach could work (NRC, Klein, 2008).

Any new commercial fuel fabrication facility supporting utilization of advanced products would be licensed under Part 70, for which NUREG-1520, “Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility,” provides regulatory guidance. However NRC may still determine whether revised regulatory requirements or additional guidance are necessary to address the recycled uranium and mixed plutonium/minor actinide feed stocks (NRC, SECY-06-0066, 2006).

In addition, the safeguards and security aspects of commercial spent fuel recycling facilities would be a significant component of the licensing review process. NRC may need to assess changes to 10 CFR Part 73, “Physical Protection and Plants and Materials” and 10 CFR Part 74, “Material Control and Accounting of Special Nuclear Material,” to account for the unique characteristics of facilities included in the advanced spent fuel recycling program. 10 CFR Part 75 would also need to be implemented to determine the international safeguards and AP requirements for the facilities (NRC, SECY-06-0066, 2006). NRC has recently issued Draft Regulatory Guides on Reporting of Safeguards Events, DG-5019, June 2007, and Managing the Safety/Security Interface, DG-5021, July 2007.

K-4. STATUS OF NRC INFORMATION EXCHANGE ON CIVILIAN FUEL CYCLE FACILITIES

The NRC hosted the third annual Fuel Cycle Information Exchange (FCIX 2008) from June 17 to June 19, 2008. The exchange was open to the public and provided an opportunity for NRC staff, licensees, and other stakeholders to present papers (see http://www.nrc.gov/public-involve/conferences.html) and discuss the regulation of civilian nuclear fuel cycle facilities. These discussions provide insight into the issues created by the current regulations from both the NRC and licensee perspective.

Since the year 2000 and for fuel cycle facilities, NRC has used a risk-informed, performance-based regulatory approach. This has employed a modification of 10 CFR Part 70 to provide increased confidence in the margin of safety, requirement of performing an ISA, Subpart H added and Standard Review Plan (NUREG-1520). The following is a timeline of Significant Occurrences Affecting Regulation of Fuel Cycle Facilities (Giiter, NRC FCIX 2008).

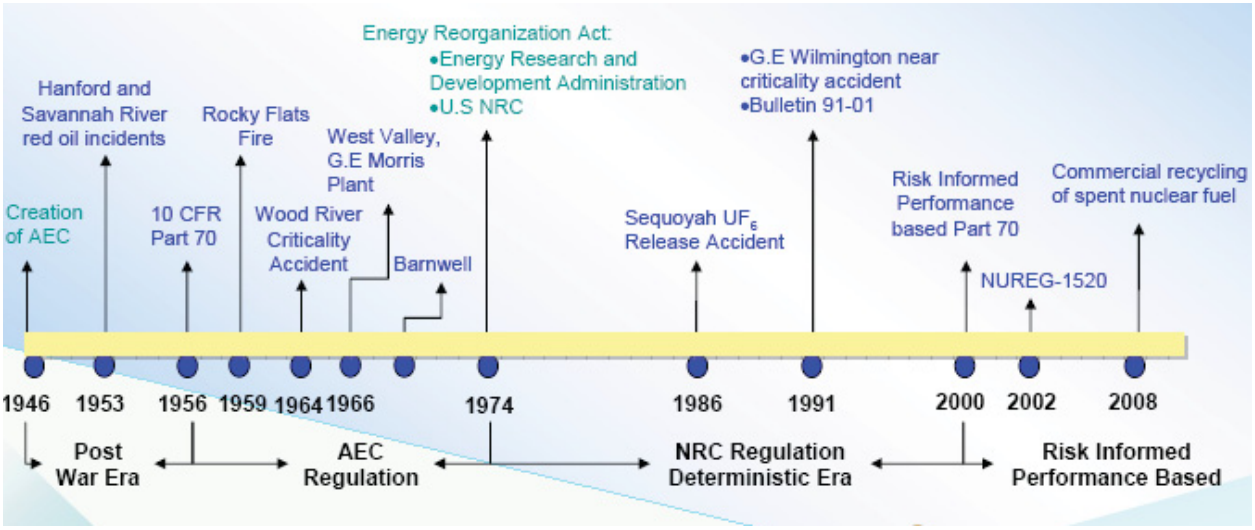


Figure K-1. Significant Occurrences Affecting Regulation of Fuel Cycle Facilities – NRC FCIX 2008 paper #3, Evolution of the 10 CFR Part 70, J. Giitter & M. Gonzales, NRC, Division of Fuel Cycle Safety and Safeguards.

Regarding new fuel cycle facilities, the following are now expected for license application in the United States:

- Uranium Enrichment - 2 facilities under construction and 2 more applications expected – Louisiana Energy Services, National Enrichment Facility gas centrifuge plant at Lea County, NM; USEC American Centrifuge Plant at Piketon, OH, GE-H planning an application this year for a full-scale laser U enrichment facility at Wilmington, NC and AREVA planning gas centrifuge enrichment plant in ID
- Mixed Oxide Fuel Fabrication Facility - Construction permit issued; operating license review – Savannah River
- Uranium Recovery - 20 new applications comprising mainly in-situ leach (ISL) and some conventional mines plus 10 restart/expansion applications (ISL and conventional)

- Spent fuel reprocessing – potential plant, consolidated fuel treatment center (CFTC) for industry/DOE and being outlined by GNEP Deployment Studies by INRA, EnergySolutions, GE-Hitachi, Atomics International led industrial consortia.

For the fuel cycle recent progress in enhancing safety and security has been summarized as follows:

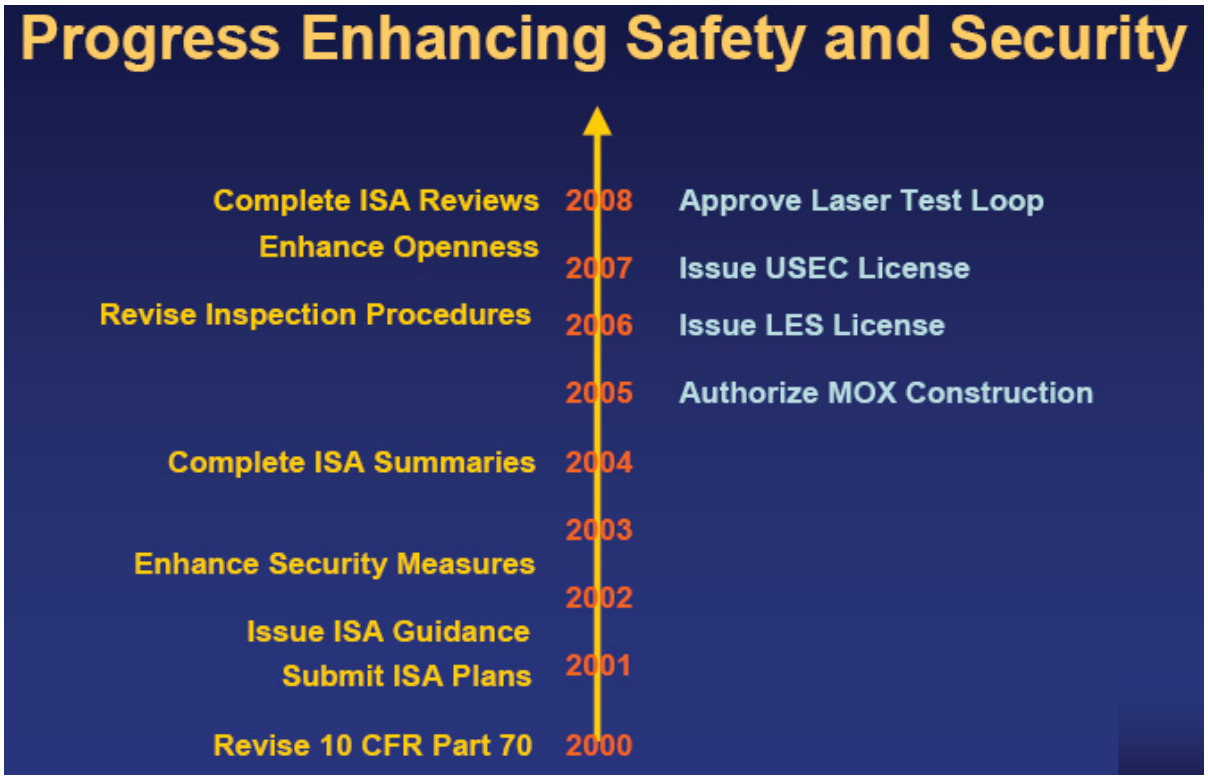


Figure K-2. Progress Enhancing Safety & Security – NRC FCIX 2008 paper #32. Fuel Cycle Regulatory Program – Meeting Challenges, Charting Path Forward, M. Weber, NRC, Nuclear Material Safety and Safeguards

K-4.1 New Enrichment Facilities

The status of U.S. enrichment plant regulation is that Louisiana Energy Services, National Enrichment Facility received COL from NRC (Parts 40 & 70) in 2006 for NM and USEC received COL for ACP in 2007 for OH. AREVA and GE-H have selected sites and will apply for COLs.

As an example, USEC's application for the American Centrifuge Plant has succeeded using the following schedule:

- First applicant under new 10 CFR Subpart H for Lead Cascade – license issued in 2004 after 12 month review; NRC prepared Safety Evaluation Rep (SER) & EA.
- License application for U Enrichment Facility (ACP) submitted August 2004 with 30 month review schedule.
- Standard application format: NUREG-1520 (Std Rev Plan), NUREG-1748 (Env Rev Guide), NUREG-1513 (ISA Guide), etc.
- EIS April 2006, SER Sept 2006, Oral before NRC Jan 2007, Hearing March 2007, ASLB decision April 13, 2007 – Construction commenced May 2007.

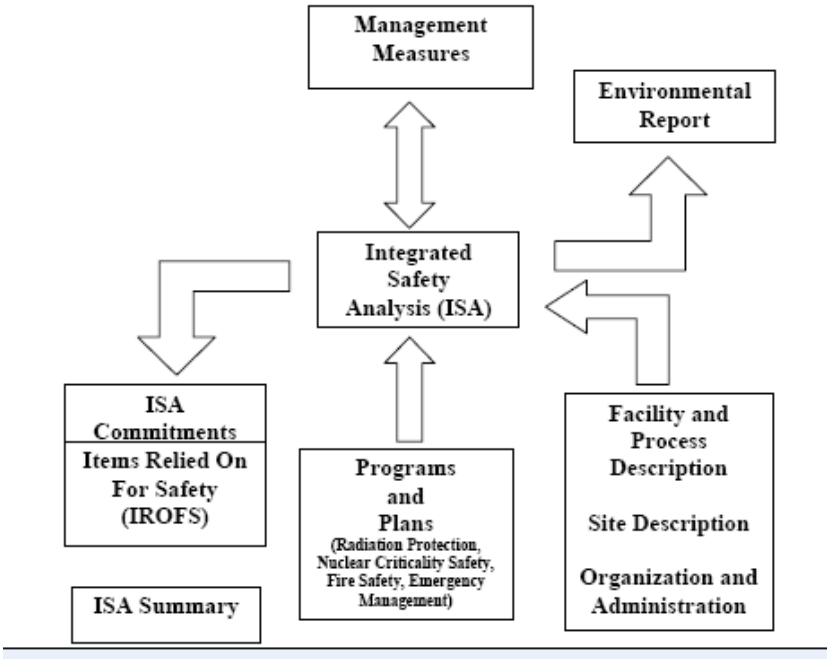


Figure K-3. Key Success Factors - NRC FCIX 2008 paper #6: USEC's American Centrifuge Issues Related to Licensing of New Enrichment Facilities, P. Miner, Director, Regulatory and Quality Assurance, USEC Inc.

K-4.2 New In-Situ Leach Uranium Recovery

- NRC received 3 new In-situ Leach (ISL) applications and expect 25 more in FY-08-FY-11
- Generally a 2 year process with issues on number of new applications, NRC staffing and interactions of stakeholders
- Developing ISL rulemaking in progress
- Key to success: Pre-applicant interaction, Limited Revisions/Amendments, EIS/SER completed on schedule, Licensing Board certify policy decisions to NRC

K-4.3 New/Relicensed Conversion/Deconversion Facilities

- Part 40 lacks detail, lots regulatory creep, No backfit rule (unlike parts 50 & 70)
- ISA Lessons Learned, by Honeywell – Metropolis, IL where UF6 conversion facility constructed in 1958
- licensed under 10 CFR Part 40 with limited ISA - License issued for a 10-year term; renewed in May 2007
- NRC may require Part 70, Subpart H ISA as aimed at new and current licensees, ~$6M cost.

K-4.4 New Reprocessing Facilities

In their GNEP Deployment study for DOE, EnergySolutions have proposed the following new licensing approach:

- Amend 10 CFR Part 50 for licensing reprocessing plants under part 70

- Use combined licensing process with inspection, tests, and acceptance criteria for COL
- Utilize a risk-informed, performance-based approach based on Part 70 model
- Regulations flexible to address various technologies
- Need standard review plan similar to NUREG -1718, SRP for MOX Fuel.

INRA (AREVA et al) describes their recommendations for application for licensing for the CFTC facility.

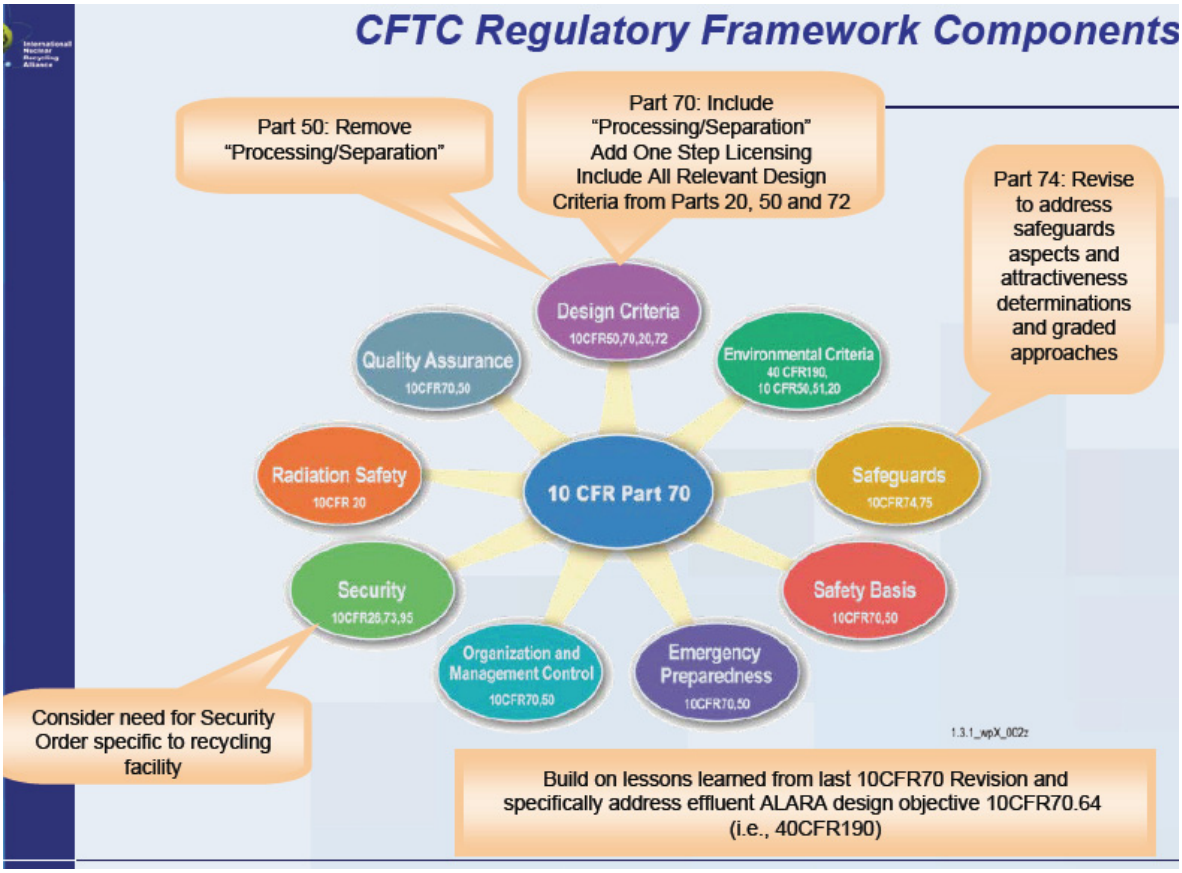


Figure K-4. 10 CFR 70 INRA Recommendation on Recycling Facility and Licensing Strategy program from D. Davidson, NRC FCIX, 2008.

It is noted that both EnergySolutions and INRA favor a one-step combined, (i.e., construction and operating) license (COL) for recycling plants as modeled on the established position for commercial nuclear power facilities.

At FCIX 2008, Dale Klein, NRC Chairman, stated that industry must increase its commitment to recycling before NRC would devote more resources toward establishing a licensing framework. Tennessee Valley Authority (TVA) is working with the Nuclear Energy Institute (NEI) to develop an approach for rulemaking in the area of nuclear fuel recycling with the objective of a proposal to NRC on where and how to move forward with establishing the regulatory framework for this (Bhatnagar, 2008).

K-5. ADAPTING THE SBD PROCESS TO NRC ENVIRONMENTS

In program and project management, DOE Order 413.3A, by the DOE including the NNSA, the main objective concerns the acquisition of capital assets with the goal of delivering projects on schedule, within budget, and fully capable of meeting mission performance, safeguards and security, and environmental, safety, and health standards. This reflects DOE's normal application of prescriptive and standards-based approaches mandating compliance with DOE directives from project outset.

The NRC has a different role as shown in the Atomic Energy Act of 1954, as Amended in NUREG-0980 – "The Act requires that civilian uses of nuclear materials and facilities be licensed, and it empowers the NRC to establish by rule or order, and to enforce such standards to govern these uses as "the Commission may deem necessary or desirable in order to protect *health and safety and minimize danger to life or property*." The NRC is not directly concerned with efficiency, production, etc., but only with regulation. There is the concern within the NRC that the regulations should not be a burden, or unattainable by the licensee. There is a move in the NRC toward risk-informed and performance-based regulations. Many of these are favored by industry for perceived more effective use of resources. In summary, the NRC formulates policies, develops regulations governing nuclear reactor and nuclear material safety, receives license applications, issues licenses, oversees operational experience, makes orders to licensees, oversees enforcement, adjudicates legal matters and conducts research and risk assessment. Most regulatory emphasis is presently about new reactors types, sites and construction but the only new civilian nuclear facilities are under construction today are fuel cycle ones.

For example, the SBD process generates various reports arising from Safeguards Design Activities at the Initiation to Transition/Closeout phases. One of these, the vulnerability assessment report (VAR), arises from the DOE requirements/guidance for conducting vulnerability assessments, which is provided in Section E (and its appendices) of DOE Manual 470.4-1. The process of conducting a VA includes gathering data that describe the physical and operational characteristics of a Safeguards and Security system, assigning values such as delay and detection, and analyzing the results to determine the relative effectiveness in conjunction with the adversary's capabilities as identified in the DBT and the Adversary Capabilities List. Section E of M 470.4-1 identifies issues that must be considered in modeling and Section E, Appendix 2, identifies an extensive list of modeling tools approved by DOE. The Manual also provides information about other mandatory safeguards and security planning documents.

In contrast, the NRC does not require licensees to perform specific vulnerability assessments in the same manner as DOE but NRC does incorporate physical protection through consideration of the following process. There is a requirement in 10 CFR 73.46(b)(4) for performance tests (mainly security personnel training, equipment and qualification) that the NRC employs, in combination with meeting the prescriptive requirements in 10 CFR 73.45 (mainly protective force, barriers, detection, training, organization) and 10 CFR 73.46 (mainly physical protection systems, sub-systems, components and procedures) and expert judgment to verify that fuel cycle facilities meet the performance requirements in 10 CFR 73.20 (General performance objectives and requirements). For reactor facilities, the corresponding performance testing requirement is in 10 CFR 73.55(b)(4) and the general and specific performance requirements are contained in the remainder of 10 CFR 73.55. None of this requires the preparation of a formal vulnerability assessment; although 10 CFR 73.55 requires the identification of reactor facility vital areas which is typically accomplished using a fault tree analysis approach.

Earlier discussion, Volume 1, Section 6, assumes that DBAs will be needed for the safety analysis and DBTs for the PP analysis of the facility. This assumption may be less appropriate for the risk-informed approach within the commercial sector as it may constrain the SBD process needlessly to a prescriptive design and regulatory treatment. A problem with using DBAs in a novel facility is that they are difficult to formulate wisely. The DBA approach works best in dealing with the n-th of a kind facility, where its vulnerabilities are well understood. With novel facilities such an understanding is typically yet to be learned. Thus, the opportunities for poorly informed prescriptions are abundant. The SBD treatment

is risk-informed, and lends itself to a design approach where successive system performance analyses are used to guide a process of steady design improvement. In this process, results of analyses of the latest iteration upon a facility design are used to identify the remaining most important performance weaknesses. In the next design iteration these are then improved upon, until the design reaches an acceptable condition. In this way, use of DBAs and DBTs is less important, and may hinder evolution of the best designs.

It can be seen by the above description and detailed study of the directives and regulations that the DOE approach is the more prescriptive, which facilitates institutionalization of processes perceived as important by NNSA and DOE NE.

This suggests a first possible approach that NRC licensees, for example nuclear utilities, and their contractors, e.g., reactor vendors, architect-engineers and comprehensive engineering, procurement, construction, operations and maintenance organizations, will most benefit from the application of the techniques proposed by the SBD processes. Increasing general industry emphasis on Front End Loading process for good project definition and control and Value Management process for proactive, problem-solving/seeking service to maximize functional value by managing project development from concept to use, suggests possible receptiveness by licensees and contractors. This is consistent with experience indicating that early adoption of the safeguards requirements and principles into the design process will be the most cost effective approach as described elsewhere in this document. But a difficulty of such a gradual "diffusion" approach is the diversity and large numbers of potential users and the reliance on a less direct approach to institutionalizing SBD in the commercial sector.

A second and intermediate approach is to encourage the prudent licensee to have frequent communication and information exchange, including regarding SBD, with the NRC for several reasons:

- The first is that the regulator will be able to learn about the process as the design develops
- The regulator will have an opportunity to comment on the design and safeguards aspects at an early stage and to affect design to make it more licensable
- The regulator can develop any new regulation and standard review plans once the design is finalized and hopefully prior to the construction
- The regulator will be more likely to approve the operating license when the design and controls are understood.

These principles were demonstrated by the development of Risk-Informed Inspection (RII) by the ASME Research Committee on RII. Industry, NRC, Nuclear Utilities, the Electric Power Research Institute and consultants worked together to develop the techniques to implement RII (Phillips, 2005). These techniques included use of:

- Probabilistic risk assessment (PRA)
- Quantitative or qualitative approach
- Plant engineering knowledge – expert judgment
- Risk importance measures used – average contribution, risk reduction and achievement worth.

By the time industry and the nuclear utilities were ready to implement RII, the NRC regulators had developed the standard review plans necessary to review specific RII programs developed for the nuclear power plants.

A third and possibly shortest route is to seek to influence directly the appropriate (Draft) Regulatory Guide and/or standard format and content of license applications to NRC with the objective of identifying the potential use of a design methodology with early integration of safeguards design within the overall design process, for example SBD. Although applicants have the freedom to make their application to

NRC using preferred design methodologies and in any written manner they wish, it is generally acknowledged that effective and economical applications and timely approvals of good cases stem from good compliance with NRC standard format and content of the application.

For example, a recent successful applicant for a fuel cycle facility license identified various key success factors including (NRC, Miner, 2008):

- Application followed standard format and content
  - NUREG-1520, Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility
  - NUREG-1748, Environmental Review Guidance for Licensing Actions Associated with NMSS Programs
  - NUREG-1513, Integrated Safety Analysis Guidance Document
  - Other NRC Regulatory Guides, other documents and industry standards
  - Standard submittal format facilitates a uniform and clear presentation
- Standard Review Plans provide guidance on NRC review and acceptance criteria
- Prompt response for requests for additional information
- Adherence to very structured environmental review process – EIS – NEPA, 1969
- Company preparation of Compliance Matrix for standard format and content.

K-6. SUPPORT TO ISBD BY GEN IV PR & PP METHODOLOGY AND INTEGRATED PROLIFERATION RESISTANCE ANALYSIS

A process, Integrated Proliferation Resistance Analysis (IPRA), for the integration of safeguards into commercial facility design has been proposed (Kovacic and Morgan, 2008). It has the goal of strengthening proliferation resistance by developing a formalized process for ensuring proliferation resistance and safeguards are adequately addressed during the early stages of facility design, integrating intrinsic and extrinsic proliferation resistance features into the design of nuclear facilities and institutionalizing the IPRA process. IPRA discusses the “flow-down” of design criteria and requirements and the integration of proliferation resistance design and analysis during the overall facility design to provide satisfactory detailed design, and facility construction and operation. This methodology, which is modeled on the approach utilized by the NRC (USNRC, Integrated Safety Analysis Guidance Document, NUREG-1513, 2001) to integrate safety into the design and operation of nuclear facilities, may have applications that could be utilized to support the ISBD project. This is pre-dated by a related PR evaluation methodology developed by the Gen IV PR group deriving from accepted nuclear facility safety evaluation methodologies (Zentner and Bjornard 2006). An example of design approaches for reducing the proliferation risks of gas centrifuge enrichment plants has been provided by a collaboration of four National Laboratories (ORNL, March 2006).

An ISA is a systematic and documented examination of a facility's processes, equipment, structures, and personnel activities to ensure that all relevant hazards that could result in unacceptable consequences have been adequately evaluated and appropriate protective measures have been identified. An ISA is known in the chemical industry as a process hazard analysis. The final rule, 10 CFR Part 70 (Domestic Licensing of special nuclear material), includes a requirement that certain licensees/ applicants subject to 10 CFR 70 conduct an ISA. Generic techniques, similar to ISA, have been applied in DOE and commercial nuclear fuel processing plants for several decades.

K-7. CONCLUSION

This appendix outlines the status of NRC process for regulation of commercial nuclear power facilities and for non-reactor nuclear facilities. It shows the predominance of combined license applications for nuclear power facilities and the emphasis by vendors on introduction of COLs for any new reprocessing facilities in the U.S. It describes recent progress concerning the potential licensing of advanced commercial spent fuel recycling facilities as envisaged by DOE and the GNEP deployment studies issued by several industrial consortia. The status of information exchange on civilian fuel cycle facilities is summarized by abstraction from the NRC FCIX, which took place during June 17-19, 2008 at Rockville, MD.

This appendix uses the above and other information to identify three potential approaches for adaptation of the SBD process to the NRC environment. These are as follows:

1. Widespread dissemination and promotion of the SBD process to NRC licensees and their contractors and sub-contractors.
2. Encouragement of frequent communication and information exchange, especially regarding SBD, between licensees and the NRC.
3. Direct approach to NRC with a view to seeking NRC to modify its appropriate (Draft) Regulatory Guide and/or standard format and content for license application with the objective of identifying the potential use of a design methodology with early integration of safeguards design within the overall design process, for example, SBD.

A fourth possibility is to seek parallels with or support from GEN IV PR methodologies and the IPRA process, for the integration of safeguards into commercial facility design, which is directly modeled on the approach utilized by the NRC to integrate safety into the design and operation of nuclear facilities (USNRC, Integrated Safety Analysis Guidance Document, NUREG-1513, 2001).

Appendix L

Volume 2 References

Appendix L

Volume 2 References

10 CFR Part 11, Criteria & Procedures for Determining Eligibility for Access to or Control over Special Nuclear Material.

10 CFR Part 40, Domestic Licensing of Source Materials.

10 CFR Part 50, Domestic Licensing of Production and Utilization Facilities.

10 CFR Part 52, Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants.

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 U.S./IAEA Agreement.

10 CFR Part 95, Facility Security Clearance and Safeguarding of National Security Information and Restricted Data.

Bhatnagar, A., New Build Monitor, Volume 27, No. 39, p. 9, September 29, 2008.

Bunn M., "Proliferation-Resistance (and Terror- Resistance) of Nuclear Energy Systems," lecture, Managing the Atom Project, Harvard University, "Systems Analysis of the Nuclear Fuel Cycle," Massachusetts Institute of Technology, May 1, 2006.

Carlson R. L., Integrated Safeguards: A 1988 Perspective, J. Nuclear Materials Management, pp. 10-19, January 1989.

DOE Additional Protocol Web Site, https://www.ap.doe.gov

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

DOE G 226.1-1, Safeguards & Security Oversight & Assessments Implementation Guide, 12/21/2007.

DOE G 413.3-1, Managing Design and Construction Using Systems Engineering for Use with DOE O 413.3A, 9-23-08

DOE G 413.3-11, Project Management Lessons Learned, 8-5-08

DOE G 413.3-3, Safeguards and Security for Program and Project Management, 11-15-07.

DOE G 413.3-9, Project Review Guide for Capital Asset Projects, 9-23-08

DOE G 420.1-1, Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria Guide for use with DOE O 420.1 Facility Safety, 03/28/2000.

DOE G 420.1-2, Guide for the Mitigation of Natural Phenomena Hazards for DOE Nuclear Facilities and Non-Nuclear Facilities, 03/28/2000.

DOE G 420.1-3, Implementation Guide for DOE Fire Protection and Emergency Services Programs for Use with DOE O 420.1B, Facility Safety, 09/27/2007.

DOE G 450.4-1B, Volume 1, Integrated Safety Management System Guide, 03/01/2001.

DOE M 142.2-1, Manual for Implementation of the Voluntary Offer Safeguards and Additional Protocol with the IAEA, Approved: 9-4-2008.

DOE M 205.1-3, Telecommunications Security Manual, 04/17/2006.

DOE M 205.1-4, National Security System Manual, 03/08/2007.

DOE M 413.3-1, Project Management for the Acquisition of Capital Assets, 03/28/2003.

DOE M 470.4-1 Chg 1, Safeguards and Security Program Planning and Management, 8-26-05.

DOE M 470.4-2 Chg 1, Physical Protection, dated 8-26-05.

DOE M 470.4-3 Chg 1, Protective Force, dated 8-26-05.

DOE M 470.4-4, Information Security, dated 8-26-05.

DOE M 470.4-5, Personnel Security, dated 8-26-05.

DOE M 470.4-6 Chg 1, Nuclear Material Control and Accountability, dated 8-26-05.

DOE M 470.4-7, Safeguards and Security Program References, Office of Security and Safety Performance Assurance, dated 8-26-05.

DOE NNSA, Next Generation Safeguards Initiative (NGSI), nnsa.energy.gov/news/print/1912.htm.

DOE O 142.2A, Voluntary Offer Safeguards Agreement and Additional Protocol with the IAEA – NNSA, Approved: 12-15-06 (NA).

DOE O 205.1A, Cyber Security Management, 12/04/2006.

DOE O 226.1, Implementation of DOE Oversight Policy, 9-15-05.

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

DOE O 420.1B, Facility Safety, 12/22/2005.

DOE O 425.1C, Startup and Restart of Nuclear Facilities, 03/13/2003.

DOE O 461.1A, Packaging and Transfer or Transportation of Materials of National Security Interest, 04/26/2004.

DOE O 470.2B, Independent Oversight and Performance Assurance Program, 10/31/2002.

DOE O 470.3A, *Design Basis Threat Policy* (U), 11/29/2005.

DOE O 470.4A, Safeguards and Security Program, 05/25/2007.

DOE O 5660.1B, Management of Nuclear Materials, 05/26/1994.

DOE P 205.1, Departmental Cyber Security Management Policy, 05/08/2001.

DOE P 410.1A, Promulgating Nuclear Safety Requirements, 05/15/1996.

DOE P 413.1, Program and Project Management Policy for the Planning, Programming, Budgeting, and Acquisition of Capital Assets, 06/10/2000.

DOE P 470.1, Integrated Safeguards & Security Management (ISSM) Policy, 5-08-01.

DOE-STD-1189-2008, Integration Of Safety Into The Design Process, March 2008.

Durst P.C., Advanced Safeguards Approaches for New Reprocessing Facilities IAEA/JAEA Workshop – Tokai-mura, Japan, November, 2007.

Eisner H., Essentials of Project and Systems Engineering Management, 2nd Edition, Wiley, 2002.

GAO, United States Government Accountability Office, Report to Congressional Committees, Weapons of Mass Destruction – Nonproliferation Programs Need Better Integration, GAO-05-157, January 2005.

Gen IV, Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems, The Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group, GIF/PRPPWG/2006/005, Revision 5, pp. 65-69, November 30, 2006.

Global Nuclear Energy Partnership (GNEP), 30% Conceptual Design Report for the Advanced Fuel Cycle Facility (AFCF), DOE Office of Nuclear Energy, January 26, 2007.

Golay, M.W., Risk-informed Operational Decision Management (RIODM): Risk, Event Trees and Fault Trees, Fall 2005, Lecture 1, Massachusetts Institute of Technology, http://ocw.mit.edu/NR/rdonlyres/Nuclear-Engineering/22-38Fall-2005/59146701-17E5-442F-A9A8-559A20C198EC/0/sec1_1.pdf

Health and Safety Executive (HSE, UK), Report of the investigation into the leak of dissolver product liquor at the Thermal Oxide Reprocessing Plant (THORP), Sellafield, notified to HSE on 20 April 2005, *www.hse.gov.uk/nuclear/thorpreport.pdf* , published February 2007.

IAEA, Carlson, J., The safeguards revolution - where to from here?, on behalf of SAGSI (Standing Advisory Group on Safeguards Implementation), Paper presented to IAEA Safeguards Symposium, Vienna, 16-20 October 2006.

IAEA, Department of Safeguards: Safeguards Manual – Parts SMI and SMC, Safeguards Criteria and Annexes, Vienna, Austria, January, 2004.

IAEA, Department of Safeguards: SGTS/TIE Policy Paper #20, "Joint Use of Safeguards Equipment between the IAEA and an External Party," Vienna, Austria, April 20, 2006.

IAEA, Design Information Questionnaire, Form N-91, June 2005 *www.nrc.gov/reading-rm/doc-collections/forms/iaea_n91.pdf*.

IAEA, Development of the Safeguards Approach for the Rokkasho-mura Reprocessing Plant, S. J. Johnson et al., IAEA-SM-367/8/01R.

IAEA, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual - Proliferation Resistance, Volume 5 of the Final Report of Phase 1 of the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO), 16-07-2007.

IAEA, Report of the LASCAR Forum:. Large Scale Reprocessing Plant Safeguards, IAEA, STI/PUB/922, Vienna, 1992. www-pub.iaea.org/MTCD/publications/PDF/SS-2001/PDF%20files/Session%208/Paper%208-01.pdf.

IAEA, The Structure and Content of Agreements between the IAEA and States required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons, IAEA INFCIRC/153 (Corrected), Vienna, Austria, June 1972. *www.iaea.org/Publications/Documents/Infcircs/Others/infcirc153.pdf*

IAEA,International Symposium on Nuclear Security; Safety, Security and Safeguards Interfaces (3S Concept) - determine how the 3S concept can best be implemented by the international community and as a result build confidence that nuclear energy is generated in a safe, secure and proliferation resistant manner.Vienna, Austria, 30 March–3 April, 2009. http://www-pub.iaea.org/MTCD/Meetings/PDFplus/2009/cn166/cn166_Announcement.pdf

IAEA: IAEA Safeguards Glossary – 2001 Edition, "Subsidiary Arrangements and Facility Attachments," Paragraph 1.26, and Chapter-3, "Safeguards Approaches, Concepts and Measures," Vienna, Austria, 2002.

International Council on Systems Engineering (INCOSE), Systems Engineering Handbook, A Guide for System Life Cycle Processes & Activities, Version 3.1, INCOSE-TP-2003-002-03.1, Edited by C. Haskins, August 2007.

Kovacic D. and Morgan J., INMM 49th Meeting, July 2008, IPRA which is directly modeled on the approach utilized by the NRC to integrate safety into the design and operation of nuclear facilities (USNRC, Integrated Safety Analysis Guidance Document, NUREG-1513, 2001.

NRC Regulatory Guide 1.206, Combined License Applications for Nuclear Power Plants, June 2007.

NRC, Davidson, D., 10 CFR 70 - INRA Recommendation on Recycling Facility and Licensing Strategy Program, NRC FCIX, June, 2008.

NRC, Giitter J. and Gonzales M., Evolution of the 10 CFR Part 70, NRC FCIX, June, 2008.

NRC, Klein D. E., Views on Closing the Fuel Cycle, NRC FCIX, June, 2008.

NRC, Miner P., USEC's American Centrifuge Issues Related to Licensing of New Enrichment Facilities, NRC FCIX, June, 2008.

NRC, NRO-REG-100, Draft Revision 1, "Acceptance Review Process for Design Certification and Combined License Applications," January 7, 2008.

NRC, NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, 2007.

NRC, NUREG-0980, Vol. 1, No. 6 "Nuclear Regulatory Legislation" 107th Congress: 1st Session, Published June 2002.

ENERGY REORGANIZATION ACT OF 1974

NRC, NUREG-1513, Integrated Safety Analysis (ISA) Guidance Document, 2001.

NRC, NUREG-1520, Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility, (Integrated Safety Analysis (ISA), Subpart H added).

NRC, NUREG-1718, "Standard Review Plan for the Review of an Application for a Mixed Oxide Fuel Fabrication Facility."

NRC, NUREG-1748, Environmental Review Guidance for Licensing Actions Associated with NMSS Programs.

NRC, NUREG-1860, Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing, December 2007.

NRC, SECY-06-0066, Reyes, L. A., Regulatory and Resource Implications of a DOE SNF Recycling Program, 2006.

NRC, Third annual Fuel Cycle Information Exchange, June 17 to June 19, 2008, Papers presented by NRC staff, licensees, and other stakeholders, http://www.nrc.gov/public-involve/conferences.html.

NRC, Weber, M., Fuel Cycle Regulatory Program – Meeting Challenges, Charting Path Forward, NRC FCIX, June, 2008.

NRC-DOE Next Generation Nuclear Plant Licensing Strategy, A Report to Congress, August 2008.

ORNL, Design Approaches for Reducing the Proliferation Risks of Gas Centrifuge Uranium Enrichment Plants, ORNL, LLNL, LANL, and PNNL, ORNL/TM-2006/47, Oak Ridge National Laboratory, March 2006. (Official Use Only).

Phillips, J, Risk-Informed Inspection of Nuclear Power Plants, NASA Risk Management Conference, December, 2005 http://www.rmc.nasa.gov/presentations/Phillips_Risk_Informed_Nuclear_Power_Plant_Inspection.pdf

Safeguards Assurances Incorporated (SAI): Explanatory Notes and Model Responses for (IAEA) Design Information Questionnaires, Provided by the Program for Technical Assistance to the IAEA Department of Safeguards form U.S. DOE, ISPO-24, ISPO Task C.9, May, 1979.

Wood H. G. et al., The Gas Centrifuge and Nuclear Weapons Proliferation, Physics Today, pp. 40-45, American Institute of Physics, September 2008.

Zentner M. D. and Bjornard T. A., A Comparison of the Safety Analysis Process and the Generation IV Proliferation Resistance/Physical Protection Assessment Methodology, Proc. 8th Int. Conf. on Probabilistic Safety Assessment and Management, New Orleans, LA, May, 2006.