INL/EXT-10-18751

# Facility Safeguardability Analysis in Support of Safeguards-by-Design


Philip Casey Durst
Robert Bari
Trond Bjornard
John Hockert
Roald Wigeland
Michael Zentner


July 2010


Idaho National Laboratory

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

INL/EXT-10-18751

# Facility Safeguardability Analysis in Support of Safeguards-by-Design

Philip Casey Durst
Robert Bari[1]
Trond Bjornard
John Hockert[2]
Roald Wigeland
Michael Zentner[2]

[1]BNL
[2]PNNL

July 2010

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of National Nuclear Security Administration
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

# EXECUTIVE SUMMARY

The idea of "Safeguards-by-Design" (SBD) means designing and incorporating safeguards features into new civil nuclear facilities at the earliest stages in the design process to ensure that the constructed facility is "safeguardable," i.e. will meet national and international nuclear safeguards requirements. Safeguards-by-Design has the following objectives: 1) design new civil nuclear facilities that meet national and international nuclear safeguards requirements; 2) make the implementation of safeguards at such facilities more effective and efficient; 3) avoid the costly and time consuming redesign and retrofit of facilities that occurs when safeguards issues are addressed after construction; and 4) design facilities in a manner that makes the diversion of nuclear material and misuse of the facility technically difficult and easier to detect. Safeguards-by-Design would reduce the overall project risk to the nuclear facility owner/operator and project design team by achieving early acceptance of the proposed facility safeguards system by the International Atomic Energy Agency (IAEA). Designing and incorporating safeguards features into the facility at the earliest stages in the design process is a major step forward, compared to the historic process of addressing safeguards issues following facility construction.

A challenge facing the project design team in implementing Safeguards-by-Design is to create an integrated, objective, and analytical methodology to: 1) evaluate nuclear facility safeguardability; 2) evaluate and optimize barriers and technical features to make the diversion of nuclear material, and misuse of the facility, more difficult and more easily detected; 3) compare and evaluate nuclear safeguards measures and facility design features and changes to enhance safeguards effectiveness and efficiency; 4) optimize the prospective facility safeguards approach proposed by the project design team.

To address these issues, the authors propose the development and demonstration of a "Facility Safeguardability Analysis" (FSA) methodology, which would be used by the project design team during the design and construction of new nuclear facilities. FSA would be a key step in Safeguards-by-Design that would link the safeguards requirements with the best practices and design of the safeguards measures for implementing those requirements. The nuclear safeguards experts would work closely with the project design team in performing FSA, to ensure that all needs and requirements of the project are met. The resultant analysis would support discussions and interactions with the national nuclear regulator (i.e. State System of Accounting for and Control of Nuclear Material – SSAC) and the IAEA for development and approval of the proposed safeguards system. FSA would also support the implementation of international safeguards by the IAEA, by providing them with a means to analyse and evaluate the safeguardability of facilities being design and constructed – i.e. by independently reviewing the FSA as performed by the design team.
Consequently, the IAEA would be able to model the performance of the proposed facility safeguards system using FSA, before the facility is even constructed.

As envisioned by the authors, FSA would include a:

- **Preliminary Diversion Path Analysis for Design Purposes -** to define nuclear material balance areas (MBAs), key measurement points (KMPs), and to evaluate the technical barriers that would mitigate the diversion of nuclear material, or potential misuse of the facility to produce undeclared nuclear materials.
- **Safeguardability Analysis** – to determine whether the nuclear facility would meet national and international nuclear safeguards requirements (i.e. based on detection goal quantity, timeliness for detecting a diversion, and net probability for detecting a potential diversion).
- **Project Risk Analysis** – to determine whether the facility design can meet the safeguards requirements and identify "hot-spots" in the design, where the ability to meet requirements with current technology is in question or at risk.
- **Cost and Tradeoff Analysis** – to determine the design, construction, and operating costs, and costs for implementing various proposed safeguards approaches and facility or process design options.

- **Analysis of Material-Unaccounted-For (MUF)** – to model the performance of the safeguards measures, prior to the completion of the facility design, in order to determine whether the measures and safeguards system proposed would meet domestic and international requirements; i.e. have the requisite accuracy and performance to detect the diversion of significant quantities of nuclear material.

As proposed, FSA would be a formal analysis performed by the safeguards experts within the project design team, working closely with all elements of that team. FSA would begin in the Pre-Conceptual Design stage, which is a major advance over the previous practice where the consideration of safeguards issues were addressed after facility construction was completed. The analysis would become more specific as the project progresses into Conceptual Design, with the specification of the safeguards system and design of the proposed major safeguards features and measures. The project design team would continue to use FSA during the design and construction process, confirming the performance of the safeguards system through the stages of Final Design and Construction. An expert elicitation process would be utilized to systematically analyze safeguardability at early stages in the design process, when there are uncertainties in the facility design and path analysis. Expert elicitation would also be used to prepare and prequalify the users of FSA, i.e. to make certain that they are versed in the use of the methodology and understand the inter-relationship and tradeoffs of the analyses.

Most of the aforementioned analyses have been used before, although the suite of analyses has not generally been used by the project design team. What is promising is that the various analyses exist and have already been demonstrated to varying degrees on previous projects, although in some cases after the facility construction was completed. Elements of FSA were recently utilized in the optimization of the design of the ACR-1000 advanced CANDU reactor by the Atomic Energy of Canada Ltd. (AECL) and in the design of the OPAL research reactor in Australia, providing reassurance that the further development of FSA is worthwhile.

As a next step, the authors recommend that the aforementioned analyses be mapped, standardized, codified, and integrated, and that procedures be developed so that the analyses can be more easily used. Where existing analyses are incomplete or not readily adaptable, they would be further developed and adapted for use by the project design team, for the purposes noted.

The authors also recommend testing FSA on a concrete test case, several of which are proposed in the following report. If the demonstration is successful, the authors recommend presenting FSA to the broader international nuclear safeguards community, the IAEA, and the nuclear industry, to support more systematic analysis and implementation of nuclear safeguards in new nuclear facilities under design and construction worldwide.

# ACKNOWLEDGEMENTS

Funding for this study and the preparation of the subject document was provided by the U.S. DOE NNSA Office of Nonproliferation and International Security (NA-24) under the Safeguards-by-Design Project, and in support of the NNSA Next Generation Safeguards Initiative (NGSI). The authors wish to thank the Office of NA-24 for their input, support, and guidance in preparing the subject report.

## CONTENTS



## FIGURES

## LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| 3S | (IAEA) Safety, Safeguards, and Security (analogous to SBD) |
| ACR-1000 | (AECL) Advanced CANDU Reactor, Model-1000 |
| AECL | Atomic Energy of Canada Limited |
| AFR | Away-from-reactor storage (of spent fuel) |
| AP | (IAEA) Additional Protocol (see also INFCIRC/540) |
| BNL | U.S. DOE Brookhaven National Laboratory |
| CA | (IAEA) Complementary Access (under the Additional Protocol) |
| CANDU | Canadian Deuterium/Uranium Reactor |
| CDR | (Project Management) Conceptual Design Report |
| CNSC | Canadian Nuclear Safety Commission |
| CofK | (IAEA) Continuity of Knowledge regarding containment (also called COK) |
| C/S | (IAEA) Nuclear Material Containment and Surveillance |
| CUMUF | (IAEA) Cumulative MUF (see also MUF below) |
| DI | (IAEA) Design Information |
| DIE | (IAEA) Design Information Examination |
| DIQ | (IAEA) Design Information Questionnaire |
| DIV | (IAEA) Design Information Verification |
| DOE | U. S. Department of Energy |
| EFL | (NWS) Eligible Facility List |
| FA | Facility Attachment |
| FSA | (NNSA) Facility Safeguardability Analysis |
| Gen-III | Generation-III Nuclear Power Plants (current generation of modern plants) |
| Gen-IV/GIF | Generation-IV International Forum (next generation nuclear energy system) |
| HEU | Highly Enriched Uranium (U-235 $\geq$ 20%) |
| HTGR | High Temperature Gas Cooled Reactor |
| HTR | High Temperature Reactor (general category) |
| IAEA | International Atomic Energy Agency |
| INFCIRC/66 | (IAEA) Early Safeguards Agreement (now limited to India, Israel, and Pakistan) |
| INFCIRC/153 | (IAEA) Model Comprehensive Safeguards Agreement |
| INFCIRC/540 | (IAEA) Model Additional Protocol |
| INL | (U. S. DOE) Idaho National Laboratory |
| INPRO | (IAEA) International Project on Innovative Nuclear Reactors and Fuel Cycles |

| | |
|---|---|
| KMP | (Nuclear material flow or inventory) Key Measurement Point |
| LANL | (U. S. DOE) Los Alamos National Laboratory |
| LEU | Low Enriched Uranium (U-235 < 20%) |
| LWR | Light Water Reactor |
| MBA | Nuclear Material Balance Area |
| MBP | (IAEA) Material Balance Period |
| MOX | Mixed Plutonium/Uranium Oxide |
| MUF | (IAEA) Material Unaccounted For |
| MWe | Megawatts, electric (electrical power output or rating) |
| NA-24 | (U. S. DOE/NNSA) Office of Non-Proliferation and International Security |
| NDA | Non-Destructive Assay |
| NGNP | (U.S. DOE/NNSA) Next Generation Nuclear Power Plant |
| NGSI | (U.S. DOE/NNSA) Next Generation Safeguards Initiative |
| NGSS | (IAEA) Next Generation Surveillance System |
| NMC&A | (U.S. DOE/NNSA) Nuclear Materials Control and Accounting |
| NNSA | (U. S. DOE) National Nuclear Security Administration |
| NNWS | (NPT) Non-Nuclear-Weapons State |
| NPT | Treaty on the Non-Proliferation of Nuclear Weapons |
| NRC | United States Nuclear Regulatory Commission |
| NU | Natural Uranium (U-235 ca. 0.71%) |
| NWS | (NPT) Nuclear-Weapons State |
| OPAL | Open Pool Australian Light Water Reactor |
| PDI | (IAEA) Person-Day of Inspection |
| PNNL | (U. S. DOE) Pacific Northwest National Laboratory |
| PP | Physical Protection |
| PRPP | Proliferation Resistance & Physical Protection assessment methodology |
| PRRA | Proliferation Risk Reduction Analysis |
| PSAR | Preliminary Safety Analysis Report |
| Pu | Plutonium, Chemical Symbol |
| Pu-239 | Prominent fissile isotope of plutonium |
| $PuO_2$ | Plutonium Dioxide (ingredient in MOX) |
| SAR | Safety Analysis Report |
| SBD | (NNSA) Safeguards-by-Design |
| SER | (U.S. NRC) Safety Evaluation Report |
| SGAR | (NNSA proposed) Safeguards Analysis Report (previously called SGER) |

| | |
|---|---|
| SGCP | (IAEA) Safeguards Division of Concepts and Planning |
| SGEE | (IAEA) Safeguards Section of Effectiveness Evaluation |
| SGO (A/B/C) | (IAEA) Safeguards Operations Division-A, B, or C |
| SLA | (IAEA) State Level Safeguards Approach |
| SNM | (U.S. DOE) Special Nuclear Material, i.e. plutonium, enriched uranium, and U-233 |
| SNRI | (IAEA) Short-Notice Random Inspection |
| SQ | (IAEA) Significant Quantity of Fissile Material |
| SRD | (IAEA) Shipper/Receiver Difference |
| SSAC | State System of Accounting for and Control of Nuclear Material (often the national nuclear regulator) |
| Th | Thorium, chemical symbol |
| TRC | (IAEA) Technical Review Committee |
| U | Uranium, chemical symbol |
| U-233 | Fissile Isotope of Uranium, bred from Thorium |
| U-235 | Fissile Isotope of Uranium |
| U-235% | Uranium Enrichment (expressed as % of uranium total) |
| U-238 | Non-fissile Isotope of Uranium in nature |
| $UF_6$ | Uranium Hexafluoride (typical feed to enrichment plants) |
| VOA | (NWS) Voluntary Offer Safeguards Agreement |

# Facility Safeguardability Analysis In Support of Safeguards-by-Design

## INTRODUCTION

Most countries have international safeguards agreements with the International Atomic Energy Agency (IAEA), concluded pursuant to signing the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). These safeguards agreements are typically patterned after the IAEA model comprehensive safeguards agreement, INFCIRC/153.[1, a] The purpose of these safeguards agreements is to provide the IAEA with the opportunity and legal mechanism to verify and ensure that nuclear material has not been diverted from nuclear facilities within the country for non-peaceful purposes. The IAEA routinely and systematically inspects Non-Nuclear-Weapons States (i.e. most countries), to verify compliance with their safeguards agreements. However, the Nuclear-Weapons States (United States, United Kingdom, France, China, and Russia) include their civil nuclear facilities on an Eligible Facility List (EFL), under a Voluntary Offer type safeguards agreement (VOA) with the IAEA. This allows the IAEA to randomly select facilities from the list for routine inspection. The purpose of this is to establish a common standard for international safeguards worldwide and to impose the same burdens and responsibilities on Nuclear-Weapon States, as Non-Nuclear-Weapon States. In principle, civil nuclear facilities operating in all of these countries are subject to the implementation of international nuclear safeguards and inspection by the IAEA – although in some cases this is routine and systematic, and in others random. The use of random inspections in the latter case is to conserve the limited resources of the IAEA. Consequently, all civil nuclear facilities should be constructed with the requirements of international nuclear safeguards in mind.

The fundamental objective of international safeguards is to detect the diversion of significant quantities of nuclear material from peaceful to non-peaceful uses, and to detect possible misuse of nuclear facilities for undeclared purposes. The specific international safeguards objectives will be described in more detail later in this report. Importantly, domestic safeguards also apply, as implemented under national regulation, and as enforced by the domestic nuclear regulator.[b] Both international and domestic safeguards require a nuclear material accounting system (i.e. nuclear material accountancy or accountability), and a means to control and verify that the accounting is correct. In the United States this is typically referred to as nuclear material control and accounting (NMC&A), while in the IAEA and internationally this is called "nuclear material accountancy." In support of nuclear material accountancy, both domestic and international safeguards apply containment and surveillance measures (i.e. video cameras, tamper indicating seals, nuclear material flow monitors, etc.) and additional measures. In the majority of cases, the domestic and international safeguards systems overlap in terms of equipment and

---

[a] Most safeguards agreements are based on the IAEA model comprehensive safeguards agreement, INFCIRC/153 (Corrected). However, three states – India, Israel, and Pakistan - have agreements based on the older INFCIRC/66, although the safeguards agreement with India is in the process of being revised to be more in keeping with the model comprehensive safeguards agreement.

[b] In the United States, the designated national authority is the U.S. Nuclear Regulatory Commission (NRC) for NRC-licensed facilities, and the U.S. Department of Energy (DOE) for DOE regulated facilities.

function. Historically, the IAEA safeguards equipment and systems were separate from those used by the operator; although the designer should provide for the installation of the equipment to accommodate international safeguards. Under Safeguards-by-Design, it is anticipated that the equipment that supports domestic and international safeguards could be more effectively integrated and shared, which should produce cost savings for both the owner/operator, national regulator, and the IAEA – although the IAEA will still need to be able to derive independent safeguards conclusions.

The implementation of nuclear safeguards in general is becoming more challenging, especially as larger and more complex nuclear facilities are designed and constructed, e.g. spent fuel reprocessing facilities, mixed plutonium/uranium oxide (MOX) conversion and fuel fabrication plants, and uranium enrichment plants. These facilities are especially of concern to the IAEA, since they handle, or can produce, fissile nuclear material, including plutonium and highly enriched uranium (HEU).

In order to implement safeguards more effectively in new nuclear facilities, the IAEA and a host of governments, organizations, and members of the nuclear industry, have proposed the idea of integrating nuclear safeguards and security provisions in the design of nuclear facilities at the earliest stages. Generically, this is referred to as "Safeguards-by-Design" (SBD). Safeguards equipment experts at AREVA/Canberra and the IAEA have also put forward the idea of integrating Safety, Safeguards, and Security features into the facility design at an early stage, a process that they have termed "3S."[2] What matters most about both of these ideas is the similarity of the vision – i.e. that more effective integration of the nuclear safety, safeguards, and security elements should occur in the design of nuclear facilities, that this integration process should address the requirements of the domestic nuclear regulatory and the IAEA, and that this should occur at a very early stage in the design process.

According to the Atomic Energy of Canada Limited (AECL), U.S. DOE/NNSA, and others, the expected benefits of implementing "Safeguards-by-Design" are that it will:[3]

- **Reduce the risk of the potential diversion of nuclear material and spread of nuclear weapons**; as the number and variety of nuclear facilities increases worldwide.
- **Reduce the cost to the IAEA of implementing safeguards**, while also increasing safeguards effectiveness.
- **Minimize project risk**; i.e. potential cost overruns and schedule delays that might result as a consequence of designing and implementing safeguards measures after construction, before the facility is allowed to start up.

The implementation of Safeguards-by-Design is described in more detail in the reference noted.[4] While the implementation of Safeguards-by-Design appears logical and compelling for the points noted, the nuclear facility designer, and Project Design Team face fundamental questions that should be addressed very early in the design process.

**These questions, which will strongly determine both the design of the facility safeguards system, and the design of the nuclear facility and process, can be summarized as follows:**

- What are the relevant safeguards requirements?
- What are the risks to the project of not meeting these requirements?
- What are the potential nuclear material diversion paths and facility misuse scenarios for the facility and/or process?
- What are the barriers that prevent the diversion of nuclear material and/or misuse of the facility for the undeclared production of nuclear material?
- What is the design of the safeguards system, to support domestic, as well as international safeguards?

- How can the facility and/or process be designed to enhance the barriers to diversion and facility misuse?
- If the facility design is altered to minimize the risk of nuclear material diversion, what are the associated tradeoffs, in terms of reduction in operating efficiency or increased cost?
- Can the facility design be optimized so that the objectives of the facility designer, owner/operator, national nuclear regulator, and the IAEA can be met simultaneously?

Historically, these questions have been addressed as the design of nuclear facilities has gradually evolved, and together with it, the implementation and evolution of international nuclear safeguards, and safeguards approaches. The process has also been aided by the fact that the majority of nuclear facilities in the world today are nuclear power plants and research reactors, in which the implementation of safeguards has been established and is generally straight forward. Essentially, the common safeguards approach for these types of facilities has followed the precedent of the safeguards approach as established by the national regulator and the IAEA.[c] This typically involved the installation of a limited number of pinpointed video surveillance systems, tamper indicating seals, and power output monitors. In most of these cases, the facility could easily accommodate installation of the IAEA safeguards equipment after the facility started up. However, with the advent of larger and more complex nuclear facilities, it has now become imperative that the installation of the safeguards equipment be anticipated very early in the design process. Otherwise, the requisite safeguards measurement accuracy, and hence, safeguards objectives, may not be attainable. In this worst case, the facility may be found to be “un-safeguardable.” For this reason the facility designer and project design team need a tool to answer the questions posed above.

In support of the facility designer, and the implementation of Safeguards-by-Design, the authors propose the integrated use of a suite of analyses and methodology that will permit the facility designer and project design team to answer the questions posed above. These analyses and methodology are referred to by the label “Facility Safeguardability Analysis” (FSA), since they will be used to determine how the facility and nuclear material within can be optimally safeguarded. What is essential is that the Facility Safeguardability Analysis be systematic, objective, analytic, versatile, and usable by the facility project design team. FSA could also be used by officials at the IAEA to confirm that the IAEA safeguards objectives can be met with the evolving design of the facility and safeguards system proposed by the designer, while the facility is being designed and constructed. As will be described, many of the relevant analyses already exist. What is necessary is that they be mapped, standardized, integrated, and adapted more effectively for the project design team to use to evaluate facility safeguardability during the project design and construction stages.

The authors further believe that the methodology developed in the Proliferation Resistance and Physical Protection Project (PR&PP), in support of the Generation-IV International Forum (GIF), can be adapted for the use of the Project Design Team to perform Facility Safeguardability Analysis (FSA). In particular, the approach used for characterizing the diversion paths, in the path analysis, is immediately applicable.

**The following report:**

- Explains what Facility Safeguardability Analysis (FSA) is

[c] Historically, the term “Safeguards Approach” has been used in the context of international safeguards, as applied by the IAEA, and has traditionally been considered “Safeguards Confidential” for internal IAEA discussion only. However, the authors use the term in a broader sense to include the designer’s proposed system and methodology for safeguarding the facility and nuclear material within. It is not possible to implement Safeguards-by-Design, unless the designer can consider and design a preliminary safeguards approach for the facility – subject to review, enhancement, and optimization by the national regulator and the IAEA.

- Explains why FSA is now necessary
- Proposes an approach for applying FSA
- Identifies what would need to be further developed
- Explains how FSA could be used by the facility designer, national nuclear regulator, and the IAEA to confirm that the facility can be optimally safeguarded
- Outlines how a Safeguards Analysis Report (SGAR) could be prepared to document the design of the safeguards system and proposed approach, and evaluate its performance based on FSA
- Recommends cases for testing, developing, and demonstrating FSA.

The subject study and associated report were funded by the U.S. DOE National Nuclear Security Administration (NNSA) Office of NA-24, in support of the NNSA Next Generation Safeguards Initiative (NGSI), to improve the effectiveness and efficiency of international nuclear safeguards.[5]

# 1. FACILITY SAFEGUARDABILITY ANALYSIS (FSA)

**As envisioned, the facility designer and/or project design team would use FSA to do the following:**

- Compare and evaluate the effectiveness of nuclear safeguards measures
- Optimize the designer's proposed safeguards approach
- Objectively and analytically evaluate nuclear facility safeguardability (i.e. the ability to meet domestic and international nuclear safeguards requirements)
- Design the safeguards system
- Compare, evaluate, and optimize barriers within the facility and process design to minimize the risk of the diversion of nuclear material
- Systematically evaluate cost and operating efficiency tradeoffs between variations in the safeguards system and facility design
- Provide a documented paper trail and foundation for the national nuclear regulator and IAEA to confirm that the proposed safeguards system and facility design will meet national regulations and international safeguards requirements.

The first challenge is that FSA should be adaptable to analysing the relatively simple case of a research reactor and the more complex case of a spent fuel reprocessing facility or MOX conversion and fuel fabrication plant. Consequently, the authors propose that FSA be built up in a structured hierarchy of modules from a suite of analytical tools, many of which currently exist as discrete elements. The benefit of FSA is that it would bring these tools and methodology together as an integrated whole, and in a systematic, rather than ad hoc, manner. This would be extremely helpful in the case of entities designing nuclear facilities in countries where there is not a well established project or systems management methodology. However, the analyses included in FSA need to be mapped, standardized, codified, and institutionalized. Large nuclear industrial design firms already perform a number of the activities noted above, as part of their design and construction process in accordance with established project management and systems engineering methods, as noted in Reference 3. However, regarding the design of the safeguards system, these activities are often ad hoc and sometimes even performed after the operating requirements have been met and the facility constructed – i.e. after the fact. Also, many of the world's largest nuclear industrial designers and constructors are in Nuclear-Weapon States, where the civil nuclear facilities have not been subject to the same level of international safeguards inspection as in Non-Nuclear-Weapon States. Consequently, these same large industrial concerns could also benefit from a better understanding of international nuclear safeguards requirements, goals, and objectives – especially if they plan to export newly designed nuclear facilities to Non-Nuclear-Weapons States. It is no longer enough for an industrial concern to assert that it knows how to design, build, and safeguard nuclear facilities. For the sake of national regulators, the IAEA, and the international community, this should be demonstrated and documented in a more systematic manner. The authors propose that this could be accomplished with FSA.

**Ultimately, it is envisioned that FSA would help the nuclear facility designer:**

- Ensure that the safeguards requirements and goals are met in the design and operation of the facility
- Provide for the timely design and incorporation of the requisite safeguards monitoring, containment, surveillance, and verification equipment and systems
- Confirm that the safeguards requirements and objectives will still be met as the facility design matures and the facility is being constructed
- Facilitate communication between the facility designer, owner/operator, national regulator, and the IAEA on those aspects of the facility relevant to nuclear material safeguards and security at a very early stage in the design process.

# 2. INTERNATIONAL SAFEGUARDS OBJECTIVES

The overarching objective of international nuclear safeguards is the timely detection of the diversion of significant quantities of nuclear material from peaceful uses, and the deterrence of such by the risk of early detection. The following specific safeguards objectives stem from the international nuclear safeguards agreement between the country and the IAEA, as noted in Reference 1. These objectives are fundamentally the same, regardless of whether the country is considered a Nuclear-Weapon State or a Non-Nuclear-Weapon State, as defined per the Treaty on the Non-Proliferation of Nuclear-Weapons (NPT). The main difference is in the implementation, as has been discussed. In both cases however, the safeguards objectives at the facility level are the same, and are as noted below.[6]

**The specific international safeguards objectives are to:**

- Detect the diversion of 8 kg of plutonium in the form of unirradiated fresh $PuO_2$ or MOX, within one month of possible diversion, or in the form of irradiated core or spent fuel, within three months of possible diversion.
- Detect the diversion of 25 kg of U-235 in the form of unirradiated highly enriched uranium (HEU, U-235 $\geq$ 20%), within one month of possible diversion, or in the form of irradiated core or spent fuel, within three months of possible diversion.
- Detect the diversion of 8 kg of U-233, bred from thorium, in the form of irradiated fuel within three months of possible diversion, or separated U-233 within one month of possible diversion.
- Detect the diversion of 75 kg of U-235 in the form of depleted, natural, or low enriched uranium (LEU; U-235 $<$ 20%), within one year of possible diversion.
- Detect the diversion of 20 tonnes of thorium within one year of possible diversion.
- Detect possible facility misuse for the undeclared irradiation and production of plutonium and/or U-233, or other undeclared nuclear activities.

The foregoing quantities of nuclear material are considered the “Significant Quantities” as defined by the IAEA for the nuclear materials noted and are also termed “SQ.”

# 3. SAFEGUARDS-BY-DESIGN

Safeguards-by-Design requires the definition of the safeguards system functional requirements simultaneously with the integrated detailed design of the facility, starting from the very earliest Pre-Conceptual Design stage. The goal is to be able to provide assurance that the facility will be able to meet safeguards goals, even at the earliest stages of design, and to continue to evaluate the expected performance of the safeguards system as the facility design progresses. It is envisioned that the pre-conceptual safeguards system would be completed in coordination with the pre-conceptual facility design, to a level of detail sufficient to reach the conclusion that the safeguards system will meet safeguards goals. If a decision is made to move forward with the facility design, concurrent development of the safeguards system will occur, sufficient to ensure that safeguards goals continue to be met. This coordinated process continues up to and through the Construction and Operation stages of the facility, so as to preclude any design or operational changes that would undermine the effectiveness of the safeguards system. For more details regarding the implementation of Safeguards-by-Design, see Reference 4.

The iterative process used in Safeguards-by-Design is shown in Figure 1. In this figure, input to the Project Design Team passes through a number of steps, in which the requirements and constraints are defined, together with the project and nuclear safeguards "threats" and vulnerabilities.

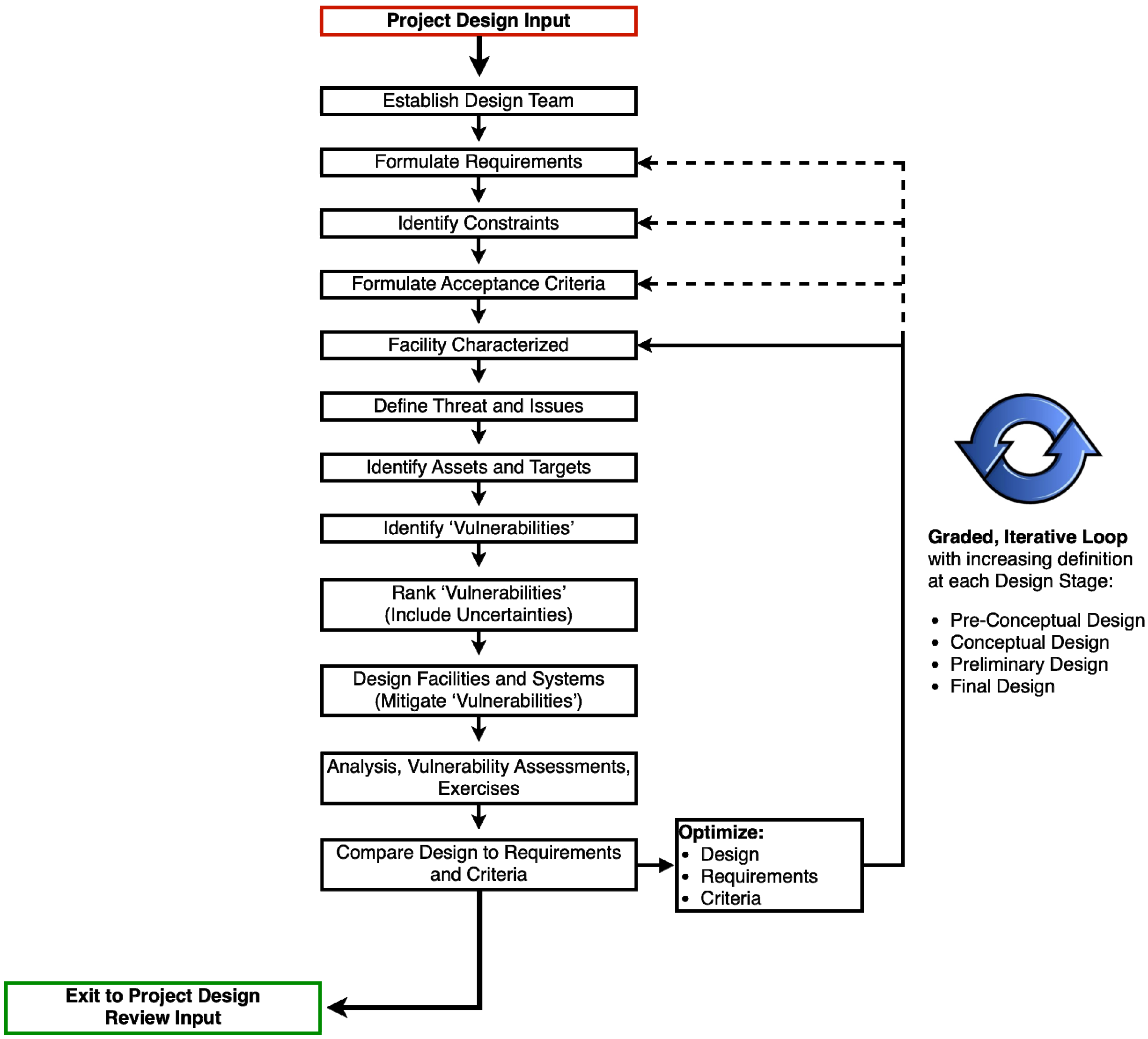


Figure 1: Safeguards-by-Design Loop
(Source – U.S. DOE Idaho National Laboratory, 2009)

Although the diagram shown as Figure 1 was taken from the report *Institutionalizing Safeguards-by-Design,* it is relevant to the process envisioned for Facility Safeguardability Analysis, since the FSA process would also be iterative and would progress through the steps as indicated.[7] The authors envision that FSA will be used at all of the major steps in the design and construction process; from Pre-Conceptual Design, through Conceptual and Final Design and Construction, up to the point of Operation.

There are fundamental overarching questions that should be answered in order to provide assurance that the safeguards system and facility design, even at the Pre-Conceptual Design stage, will meet the safeguards goals.

**These can be summarized as:**

- Can the diversion of an SQ of safeguarded nuclear material be detected in a timely manner?
- Can misuse of the facility, to produce an SQ of nuclear material, be detected in a timely manner?
- Can the diversion of nuclear material be mitigated through improved design of the nuclear facility, process, or safeguards system?

For each of these questions, as the pre-conceptual design of a facility is being developed, there needs to be a process that the designer can use to identify the design vulnerabilities for the potential diversion of nuclear material, consider options for dealing with the vulnerabilities, and evaluate the effectiveness of the proposed design solutions. The authors suggest that FSA be used to address these design issues, as outlined in the proposed approach in the next section.

# 4. A PROPOSED APPROACH FOR PERFORMING FSA

As envisioned, Facility Safeguardability Analysis would be an integrated and iterative process and methodology that would use analytical tools, many of which already exist as separate elements. All of these elements would need to be mapped, standardized, hierarchically structured, and integrated under the umbrella of FSA. The requisite input and analytical tools for the process are described as follows:

**Defining Relevant Safeguards Requirements**:

The facility designer and/or project design team would need the relevant safeguards requirements from the IAEA and national regulatory authorities. In the case of the former, the IAEA requirements stem from the safeguards objectives as described in Section 2. To meet these objectives, requirements for facility inspection, verification of nuclear material, and documentation and reporting are described in the safeguards agreement between the country and the IAEA. Additional requirements regarding the level, frequency, and accuracy of nuclear material verification are specified in the IAEA Safeguards Criteria in the *IAEA Safeguards Manual*. [8] The latter however, is an internal IAEA document and is not well known outside of the IAEA. For this reason, the U.S. DOE/NNSA has been preparing a series of *Safeguards Guidance Documents*, to better inform designers of commercial nuclear facilities of the relevant international safeguards requirements, based on the type of facility. [9, 10, 11] Domestic nuclear safeguards requirements vary from country to country. Typically, national legislation defines the nuclear regulatory requirements, with the national nuclear regulator ensuring that these requirements are met. For this reason, Safeguards-by-Design requires the involvement of both the national nuclear regulator and the IAEA. In most cases, domestic nuclear regulation provides a regulatory foundation for implementing international safeguards at domestic facilities. In general, domestic nuclear safeguards protect against the the diversion, theft, and misuse of radioactive and nuclear material. While international nuclear safeguards are directed at the timely detection of the diversion of nuclear material from peaceful purposes to non-peaceful purposes, which could potentially involve the country itself. The objectives of both, while not identical, typically overlap.

**Defining Relevant Design Information:**

To perform FSA, the facility would need to at least be at the Pre-Conceptual Design stage. The stages in the model design and construction process are described in more detail in Section 5. At this stage, the nuclear facility designer should have the:

- Nuclear Material Mass Balance Schematic
- Facility Process Flow Schematic
- Facility Pre-Conceptual Design; including identification of nuclear material entries and exits, and handling, processing, and storage areas
- Proposed Nuclear Material Balance Areas (MBAs) and Inventory and Flow Key Measurement Points (KMPs)
- Descriptions of the nuclear material chemical form(s), quantities, purity, and tentative descriptions of the nuclear material transfer, storage, and shipping containers.

It is important for the nuclear facility designer and owner/operator to recognize that this information is fundamentally relevant to the implementation of international safeguards and will be verified by the IAEA in the course of Design Information Examination and Verification (DIE/DIV), as coordinated with the constructor, owner/operator, and national nuclear regulator.

**Performing Preliminary Diversion Path Analysis (for Design Purposes):**

Preliminary diversion path analysis for design purposes, would allow the design team to quickly determine where the nuclear material would be stored, processed, and transferred in the facility for the purpose of preventing diversion of nuclear material. As part of the diversion path analysis, the Project Design Team would consider the barriers to diverting the nuclear material, as well as potentially misusing the facility. “Diversion Path Analysis” is a term used historically by the IAEA in the specific context of analyzing the nuclear material diversion paths within a nuclear facility and in the country as a whole. The authors use the term in this case, as applied by the Project Design Team, to considering and evaluating the diversion paths within the facility. This needs to be done in order to enhance diversion barriers and/or change the process and facility design to minimize the risk of the diversion of nuclear material. This can be thought of as a “Preliminary Diversion Path Analysis,” although it is recognized that the IAEA will perform an independent Diversion Path Analysis for their own purposes, typically just prior to operation of the facility. However, for Safeguards-by-Design and the use of FSA to be effective, the preliminary diversion path analysis has to be performed at the earliest stage in the design and construction process. This is a major feature of Safeguards-by-Design and FSA as envisioned by the authors. This also would require the early coordination and interaction between the IAEA Operations Divisions, the facility owner/operator, Project Design Team, and the national nuclear regulator (SSAC). It would also require that the IAEA Operations Divisions become more involved in monitoring the early stages of the design and construction process to ensure that the IAEA safeguards goals can be met, especially at nuclear facilities of novel design.

Preliminary diversion path analysis for design purposes would differ from what the IAEA performs independently. However, it is compelling for the design team to perform a diversion path analysis in order to ensure that the barriers to nuclear material diversion and facility misuse are adequate – i.e. meet national and international nuclear requirements and international nuclear safeguards objectives. From the standpoint of the design and construction project, it would allow the design team to quickly assess whether the project is potentially at risk, in terms of meeting these requirements and objectives.

Based on the pertinent facility design information and relevant safeguards requirements, the designer would perform a preliminary diversion path analysis at the Pre-Conceptual Design stage. The purpose of this would be to:

- Define the nuclear material flow and storage areas and determine from which points nuclear material could potentially be removed; including nuclear material receiving, transfer, processing, storage, hold-up, and shipping areas
- Confirm that the proposed nuclear material balance areas (MBAs) would contain all of the nuclear material to be handled, processed, or stored in the facility
- Confirm that the proposed key measurement points (KMPs) would monitor the entire flow and inventory of nuclear material
- Define the tentative location of containment, surveillance, verification, and monitoring equipment for nuclear safeguards, and how it could be optimized
- Define the nuclear material diversion barriers, and consider how they could be optimized (i.e. make the diversion of nuclear material more difficult or more easily detected)
- Determine the relationship between proposed safeguards measures and operational and safety features, potentially requiring trade-offs
- Determine if changes to the process or facility design would minimize the risk of nuclear material diversion, and perform trade-off analysis of the most relevant and promising design changes.

**The fundamental questions that the preliminary diversion path analysis would address are:**

- Can the relevant safeguards requirements and objectives be met by the facility design?
- Have all of the diversion paths been adequately identified and addressed?
- Has the tentative safeguards system been defined?
- Has the facility and process design been optimized to adequately safeguard the nuclear material handled within?

Diversion path analysis has been used within GIF, and to some extent within INPRO, and in support of U.S. DOE/NNSA projects dealing with the evaluation of Proliferation Resistance and Physical Protection (PRPP), as noted.[12] The authors believe that this tool could be used for the purposes as noted above. While FSA could be performed even during the Pre-Conceptual Design stage, the details of the proposed safeguards system and approach would become better defined as the facility design itself becomes better defined. In the course of performing the preliminary diversion path analysis, the designer would use the relevant parameters that the IAEA uses as part of their safeguards evaluation, as performed within the Section for Safeguards Effectiveness Evaluation (SGEE), in the Department of Safeguards.

**In performing the preliminary diversion path analysis, and comparison and evaluation of options, the relevant parameters are:**

- **The detection goal quantity**, i.e. the “Significant Quantity” or SQ of plutonium, uranium, thorium, U-233, and U-235
- **The goal for timely detection of a diversion** (based on whether it is so called “direct use” material, such as plutonium and HEU, and whether it is irradiated)
- **The detection probability**, (based on whether it is direct-use and whether it is irradiated)
- **Cost of the safeguards measure, approach, or design modification**

The goals for meeting international safeguards objectives are as noted in Section 2. The detection probability is prescribed by the IAEA in the aforementioned Safeguards Criteria or in the IAEA State Level Safeguards Approach (SLA). Communication with the IAEA is necessary to confirm the requisite detection probability. Cost would be used for comparing options, representing the cost in capital equipment, installation, maintenance, inspection resources, and support required to implement the safeguards measure, approach, or design change. The cost would typically be expressed in terms of $ and Person-day of Inspection Effort (PDI), although both can be combined to a net $ figure or equivalent. However, PDI is a useful metric used by the IAEA to monitor and measure field inspection effort, and consequently impact on the facility as a result of inspection effort.

By using these parameters in the scheme of FSA, correspondence will be maintained between the facility designer's systems engineering analysis, preliminary diversion path analysis, and the analysis performed by SGEE in the IAEA Department of Safeguards. In essence, the facility designer will be able to model how they expect the safeguards system to perform, while the IAEA will be able to confirm whether the safeguards requirements and goals are actually met.

An example of the use of preliminary diversion path analysis, in support of the design of a specific nuclear facility, is described in Section 7.

**Development of the Designer's Proposed Safeguards System and Approach**

Based on the relevant safeguards requirements, relevant design information, and preliminary diversion path analysis, the Project Design Team will be able to layout the prospective safeguards measures and systems, and conceive of a proposed safeguards approach. For existing facilities, this is simplified by referring to existing safeguards measures and approaches. A good example of this is presented in the reference document prepared by the IAEA for the case of future water cooled reactors, including LWRs and CANDU reactors.[13] The referenced document indicates the normal safeguards measures and the key measurement points, locations for containment and surveillance systems, and a catalog of existing approved safeguards equipment used by the IAEA for water cooled nuclear reactors. Together with this information, the facility designer will be able to formulate a prospective safeguards approach, and consider the layout of the tentative safeguards system. Communication with the IAEA at this stage is also crucial to make certain that the planned safeguards measures have not been revised or updated.

While the use of precedent is acceptable for proposing the initial design of the safeguards system and prospective approach, it is less useful for the larger, and more complex fuel cycle facilities, and other facilities of radically new design. In these cases, it is better for the designer to reduce the scope of their attention to discrete modular process units, or MBAs within the facility, and study each of these individually. If the designer approaches the design of the safeguards system for a large spent fuel reprocessing plant or MOX conversion and fuel fabrication plant in its entirety from the start, the task may be overwhelming. In this case, it would be better to analyze each MBA or process unit individually and optimize the safeguards system design and approach at that level. The analysis and approach for the individual process units would then be integrated to develop the net safeguards system design and safeguards approach. In this case, the safeguards system modules, at the level of the process units, must be compatible in terms of data collection, data transmission, and system integration.

Once the vulnerabilities have been determined, based on the preliminary diversion path analysis, the nature of the vulnerability will define the functional requirement of the needed safeguards measure; such as what needs to be measured, how well does it need to be measured, etc. The designer will be able to evaluate whether or not suitable safeguards technology exists to meet the monitoring need, or if this vulnerability represents a fundamental flaw in the project that would prevent being able to meet safeguards goals.

**Defining Safeguards System Functional Requirements:**

The results of the preliminary diversion path analysis would aid in:

- Identifying the requisite safeguards measures, which would become part of the safeguards system
- Specifying the functional requirements for the specific safeguards measures and system; i.e. safeguards monitoring, containment, surveillance, and assay systems, etc.
- Identifying the location, space, and utility requirements for the safeguards components, including power and data transmission

- Identifying areas where changes to the nuclear facility design and/or process could improve the effectiveness of the safeguards system.

The initial safeguards system would consist of safeguards measures and equipment that ideally would meet or exceed the measurement uncertainty and performance requirements, as indicated in the IAEA reference cited. [14] This reference is very important, as it provides the requisite instrument measurement accuracy, which is especially important for verifying the flow and inventory of safeguarded nuclear material in bulk handling facilities, e.g. fuel reprocessing plants, fuel fabrication plants, etc.
Of particular interest, is assessing what the most vulnerable aspects of the facility would be, in terms of safeguards, providing feedback to the designer early in the pre-conceptual design phase so that alternatives might be developed to mitigate or eliminate the vulnerability.

**Analysis of "Material Unaccounted For" (MUF):**

Based on the preceding analyses, the Project Design Team would be able to perform an initial analysis of the "material unaccounted for" (MUF) – or MUF Analysis. With a known conceptual facility design, preliminary diversion path analysis, initial safeguards system design, and known values for the performance and accuracy of the system components, the designer would be able to calculate the net measurement uncertainty for the system. At this point, the designer would be able to ascertain whether the safeguards system would be accurate enough to detect a diversion of significant quantities of nuclear material, within the prescribed timeliness of detection and detection probability. **The designer would also be able to determine if the safeguards system is marginal in meeting these requirements, and consequently if the overall project is at risk. This is the issue of fundamental importance to the facility designer, as well as the owner/operator.** Performing this analysis in advance, as part of FSA, would also give the designer insight in areas that would benefit from designing in improved measurement accuracy, redundant safeguards equipment, or even proposing additional measures to complement a single safeguards measure.

**An Iterative Process:**

The authors see the use of FSA and the integration of these analyses as iterative, as indicated in Figure 1. For nuclear facilities of a known or simple design, FSA may be largely confirmatory, based on the performance of established safeguards systems, approaches, and inspection experience. However, for large and complex facilities, and facilities of radically new design, the systematic analysis as prescribed in FSA is the only way to anticipate in advance whether the facility safeguards system would truly meet the safeguards objective. This is particularly the case for nuclear facilities of novel design, where the diversion path analysis and the development of the safeguards approach based on precedent is tenuous.

**Optimizing the Facility and Process Design and Diversion Barriers for Nuclear Safeguards:**

While the foregoing systems study type analysis has been performed in the past at the IAEA, one element that is relatively new is the freedom for the designer to use the result from this analysis as feedback to optimize the design of the nuclear facility and/or process.

As examples, the designer may consider the following:

- Processing the nuclear material in a form that remains irradiated, or not "direct-use," to minimize the so called "material attractiveness," and consequently reduce the verification and assay requirements.
- Providing for joint-use process and nuclear safeguards instruments for enhanced process control, improved nuclear criticality safety, and more effective nuclear safeguards.
- Precluding the removal of nuclear materials in the process by minimizing human and physical access, while providing controlled access to feed and product materials that require access for inventory taking.

- Systematically evaluating the interaction and potential interferences between process operation, safety, and nuclear safeguards instruments and/or activities.
- Integrating the safeguards data transmission and communication system within the instrument network in the facility in a manner that meets IAEA tamper resistance and data security requirements.
- Designing "built-in" locations for non-destructive assay (NDA) systems and detectors with custom designed shielding and collimators to optimize measurement accuracy (e.g. for precision assay of plutonium content or uranium enrichment).
- Specifying in the design the latest generation of digital video surveillance, electro-optical sealing, nuclear material accountancy, nuclear material sampling, and assay systems.
- Enhancing and using dual (two independent) nuclear material containment and/or surveillance (C/S) around MBAs containing direct-use material.
- Implementing safeguards measures and process monitoring instruments to provide additional verification of nuclear material flows.
- Designing dual (i.e. two independent) C/S systems for nuclear material in MBAs considered by the IAEA to be "difficult to access" – (e.g., such as the core and spent fuel storage areas of pebble bed modular reactors).

There are a variety of facility and process design choices that affect the implementation of nuclear safeguards. As the process and facility design evolves, changes will likely impact the safeguards system design as well. This is why the Safeguards-by-Design process is so important; to ensure the facility is in fact "safeguardable" once it is completed and meets the safeguards, as well as the operational requirements. **This is the most compelling reason for the designer to use FSA during the design process – since the design of the safeguards system for new and complex nuclear facilities is inextricably connected to the design of the nuclear facility and process, and vice versa.**

# 5. DESIGN AND CONSTRUCTION STAGES

As envisioned, the facility designer or project design team should use FSA through every stage of the design and construction process, up to the point of Operation. The convention for the design and construction stages is shown diagrammatically below, in accordance with Reference 4.*


Figure 2: Sequence of Design and Construction Stages for a Typical Project.

* There are a number of different conventions regarding the number of, and naming of design and construction stages, depending on the country and organization involved. The IAEA defines the Pre-Construction, Construction, and Commissioning phases, which correspond to the design and construction stages as noted below. Similarly, U.S. DOE defines CD-0, CD-1, CD-2, and CD-3, which are generally comparable to the stages as noted above. Regardless of the specific names, the stages are meant to represent the relative sequence and order of design and construction activities, and are comparable for the sake of this discussion.

1. **Pre-Conceptual Design** – the earliest design stage where the level of detail may only describe the functional aspects of the facility and the proposed operations, but is still sufficient to conceptually design the safeguards system. The material balance areas (MBAs) and key measurement points (KMPs) would be defined and the initial diversion path analysis performed. A preliminary FSA would be performed to determine project risk areas, in terms of meeting safeguards requirements. The designer would be able to propose a safeguards approach and safeguards system if the facility is of an established design. If the facility design is novel, then the safeguards approach and system may be proposed, but would be subject to evolution and additional refinement in later design stages.
2. **Conceptual Design -** where conceptual facility design details would be available, including proposed equipment and location along with more detailed operations planning. This would allow confirmation that the proposed safeguards system will be able to meet safeguards goals and that the facility design accommodates the locations and space required for instrumentation, monitoring equipment, etc. Hard specifications for the safeguards system would be defined, with proposed equipment locations, utility requirements, and data transmission requirements. FSA would be performed again to confirm that the safeguards requirements would continue to be met, and determine if there are potential interferences between the safeguards, plant operation, and safety systems.
3. **Preliminary to Final Design** (i.e. Design for Construction) **-** where detailed facility design, dimensions, equipment, and planned operations are specified, allowing continuing confirmation that the safeguards system will still meet specified safeguards requirements, with minimum interference with the plant operation and safety systems.
4. **Construction** – where the facility is being constructed according to the owner/operator's specification. The facility design may be changed during construction and the safeguards system must be tested to ensure that changes in facility design and/or construction have not compromised safeguards system performance. Calibration and testing of the safeguards systems typically occurs at this stage with simulated materials and/or controlled radiation sources. The performance of the safeguards system is assessed again, based on the results of these tests, prior to hot operation of the facility, i.e. introduction of radioactive material into the facility.

By applying Facility Safeguardability Analysis at each stage, the designer would have assurance that the safeguards system and facility design could meet safeguards requirements, thereby mitigating the potential risk of cost overruns because of retrofitting to accommodate safeguards, and/or a delay in facility startup.

# 6. FSA AND THE PROPOSED SAFEGUARDS ANALYSIS REPORT (SGAR)

Currently, in the licensing for the construction and operation of a nuclear power plant in the United States, a Preliminary Safety Analysis Report (PSAR) and Safety Analysis Report (SAR) are prepared to document the safety issues relevant to the nuclear facility, and how they would be mitigated and addressed by the facility design.

**The authors of this study believe that similarly, a Safeguards Analysis Report (SGAR) could be prepared by the facility designer and/or project design team to document the FSA, which would include**

- Relevant safeguards requirements
- Relevant facility design information
- Preliminary diversion path analysis and subsequent iterations
- Prospective safeguards approach proposed by the designer

- Safeguards system design
- MUF analysis
- Optimization of the facility and process design (as it pertains to safeguards)
- Trade-off analyses relevant to the optimization of the safeguards system and facility design
- Evaluation of the expected performance of the safeguards system, as validated by confirmatory testing and calibration of the safeguards equipment and components during commissioning

The latter would most likely be confirmed after the facility actually begins operation, although it would still be of great interest to the owner/operator, national nuclear regulator, and IAEA.

It is not being suggested that the SGAR become another hurdle in the licensing process for new nuclear facilities, since FSA and the proposed SGAR are still embryonic and need to be further developed. However, the idea is clearly analogous to the case of the PSAR and SAR and addressing nuclear safety issues in the design and construction of nuclear facilities. The authors suggest that something like an "SGAR" is needed to document the safeguards relevant information as noted above, for the sake of the facility designer and project design team, national nuclear regulator, and IAEA.

Another benefit of the SGAR is that it would capture the iterations of the analyses, such as the diversion path analysis, which would be performed at each major stage of design and construction. This is especially important if the original design dramatically evolves during design and construction. It would also provide traceability for the origin of the design team's proposed safeguards approach and safeguards system.

# 7. USE OF PRELIMINARY DIVERSION PATH ANALYSIS IN SUPPORT OF NUCLEAR FACILITY DESIGN – THE EXAMPLE OF AECL

It is noteworthy that Atomic Energy of Canada Limited (AECL) has applied a preliminary diversion path analysis and Safeguards-by-Design in the design of their Advanced CANDU Reactor, the ACR-1000. In so doing, AECL notes the following motivating factors for the respective parties, as paraphrased below from Reference 3:

- **For the Facility Designer** – Minimize construction cost and schedule risk (i.e., meet the safeguards requirements and complete the facility on schedule and within the allocated budget),

- **For the IAEA** – Minimize the cost of implementing international nuclear safeguards, while improving effectiveness of safeguards,

- **For the International Community** – Minimize the risk of the diversion of nuclear material from peaceful purposes, and the possible spread of nuclear weapons, as the number and variety of nuclear facilities deployed worldwide increases.

What is also significant about the case of AECL using a preliminary diversion path analysis and Safeguards-by-Design in the design of the new ACR-1000 reactor is that AECL is a nuclear reactor designer/developer and merchant supplier. Their CANDU series of reactors is subject to full-scope international nuclear safeguards inspection by the IAEA worldwide. Consequently, they have a firm understanding of the inspection goals and objectives of the IAEA, as well as the need to incorporate provisions for the safeguards measures more seamlessly in the design of the facility. They also recognize that the design of the facility itself can enhance the safeguardability. Regarding the latter, AECL has explained that the preliminary diversion path analysis especially focused attention on the design of the spent fuel handling system, spent fuel transfer canal, and storage pond. Specifically, AECL minimized personnel access to the spent fuel transfer canal, redesigned the spent fuel storage basket lids as tamper indicators, and provided space in the pond for un-stacking spent fuel baskets. This was done to allow the IAEA to more easily monitor the transfer of spent fuel from the core through the transfer canal to the spent fuel pond, and to more easily permit verification of the spent fuel in the storage baskets within the pond. This is an important precedent for the proposed application of Facility Safeguardability Analysis and further use of Safeguards-by-Design, because it shows a concrete case where a nuclear facility designer used the principles to improve the safeguardability of the facility.

The detailed interaction between the AECL project design team, the Canadian Nuclear Safety Commission (CNSC), and the IAEA was as described by Mr. Jeremy Whitlock of AECL.[15] As with any large scale nuclear design project, there was a large and complex project team, sometimes with competing interests – although all were focused on the successful completion of the design and pre-licensing of the new ACR-1000. There are a number of aspects relevant to the current discussion worth stressing as a way of example.

Firstly, the national nuclear regulator in Canada, CNSC, required that the reactor designer (AECL) implement Safeguards-by-Design and consider international nuclear safeguards issues and requirements. Although this process was not well defined, it compelled AECL to use or prepare a: 1) Design Guide to Facilitate Safeguards, 2) Preliminary Diversion Path Analysis (for design purposes), and 3) Preliminary Safeguards Approach. According to Mr. Whitlock, this was then used to assess and rank the potential nuclear material diversion pathways, using the methodology employed in the PRPP studies. The AECL Project Design Team focused on the diversion paths associated with the main areas for storing and handling nuclear fuel – i.e. fresh fuel receiving and storage, the reactor core, and the spent fuel receiving pond, transfer canal, and storage pond.

The diversion of irradiated direct-use material (i.e. irradiated plutonium in spent fuel) was considered the greatest diversion threat, based on the lower detection goal quantity of 8 kg Pu and the relatively short detection timeliness goal of three months. Consequently, the safeguards design efforts focused on: ensuring continuity of knowledge of the spent fuel discharged from the reactor to the receiving pond, and subsequent transfer to the spent fuel pond; designing the spent fuel pond with additional space to permit random selection and verification of spent fuel; etc. The active role of a safeguards expert on the design team, in this case, Mr. Whitlock, was crucial in ensuring that the IAEA safeguards requirements were met and understood by the project design team.

Secondly, Mr. Whitlock, with the approval of CNSC, facilitated additional communication with the IAEA Safeguards Operation Division-B (SGOB), responsible for implementing IAEA safeguards in Canada. Mr. Whitlock brought to the IAEA's attention those features of the ACR-1000 that were significantly different from the earlier generation of CANDU reactors – specifically the fresh fuel storage, spent fuel discharge, spent fuel storage, and spent fuel transfer to interim dry storage. This permitted informal and formal communication between AECL, CNSC, and the IAEA, which resulted in the redesigned equipment and features of the ACR-1000 that would make it easier to safeguard – i.e. make it easier to verify the fresh and spent fuel and easier to monitor the discharge of spent fuel from the core to the receiving and spent fuel ponds.

Although the example set by AECL did not follow exactly the systematic FSA process currently being proposed by the authors, it did exhibit the following proposed under Safeguards-by-Design and FSA, including:

- Establishment of a requirement by the national nuclear regulator to include Safeguards-by-Design and consideration of international nuclear safeguards in the early design stages of the facility.
- Active involvement of international nuclear safeguards experts on the project design team.
- Early definition of IAEA safeguards requirements for the project design team.

- Active and early communication between the project design team, national nuclear regulatory, and the IAEA – especially with the IAEA Operations Division responsible for safeguarding the country and facility.

- Preliminary diversion path analysis (for design purposes) to prioritize safeguards-related design efforts and to determine potential risks to the project (in not meeting safeguards requirements).

- Selective design optimization and trade-off analysis between safeguards requirements and operational efficiency issues (e.g. providing additional space in the spent fuel pond to facilitate random verification of spent fuel baskets by the IAEA while also maximizing the stacking and storage density of spent fuel).

- Preparation of a proposed safeguards approach by the project design team for the ACR-1000, considering the IAEA safeguards approach as applied to current generation of CANDU reactors, being mindful of differences between the facility designs and the implications in meeting safeguards requirements.

# 8. INTERACTIONS WITH THE IAEA

While interaction with the IAEA is proposed at the earliest stages of conceptual design, it is also important to target the interaction for maximum benefit and effectiveness. The IAEA consists of six major Departments.[16] Historically, the most involved has been the Department of Safeguards, although the roles of the Departments of Nuclear Safety and Security and Nuclear Energy are also becoming more important in providing guidance in the design of new nuclear facilities. What is important to understand is that if the nuclear facility is going to operate in a Non-Nuclear-Weapon State, (i.e. most countries), then it will be subject to full-scope international nuclear safeguards and routine inspection by the IAEA, in accordance with their international safeguards agreement with the IAEA. For this reason, the facility must be able to accommodate the IAEA's nuclear safeguards measures and approach. Consequently, this must be considered in the design of the nuclear facility. To minimize possible delays and disruptions in the facility design and construction, this should be at the earliest stages of conceptual design, in accordance with Safeguards-by-Design. Even in Nuclear-Weapon States (i.e., the United States, United Kingdom, France, China, and Russia), most civil nuclear facilities are placed on an Eligible Facility List (EFL), under a Voluntary Offer type of safeguards agreement (VOA), and are subject to random selection and inspection by the IAEA. Additionally, nuclear reactors and facilities that are designed and marketed by suppliers in Nuclear-Weapon States would be subject to international safeguards by the IAEA, if built in a Non-Nuclear-Weapon State. All of this simply emphasizes the need for new nuclear facilities to be built in accordance with Safeguards-by-Design. To facilitate this process, the authors recommend that this process incorporate an analysis of the facility safeguardability using FSA, and early involvement of the IAEA and the domestic nuclear regulator.

In terms of involving the IAEA Department of Safeguards, historically the division most involved has been Concepts and Planning (SGCP), since the idea of Safeguards-by-Design, and the related idea of "Safety, Security, and Safeguards" (3S), were new concepts. However, as nuclear facilities are actually being designed the Facility Safeguardability Analysis, and safeguards approach proposed by the facility designer or project design team, will most likely be reviewed by the respective Division of Operations – SGOA, SGOB, or SGOC - depending on where in the world the facility would be built. Once safeguards data is collected by IAEA inspectors, the data will be analyzed by the Section of Safeguards Effectiveness Evaluation (SGEE) to determine if the IAEA's safeguards goals for the facility and country are met annually.

Consequently, the IAEA Safeguards Divisions of SGCP, SG Operations, and Section of SGEE could all potentially be involved in the Safeguards-by-Design process, and potentially as reviewers of the

Facility Safeguardability Analysis. For the sake of efficiency, the Department of Safeguards may nominate a single representative, or they may adopt a team approach, as they have internally in the form of the Technical Review Committee (TRC). In any event, the interaction with the IAEA on this subject will need to broaden beyond the current dialog and involvement with personnel from SGCP, for Safeguards-by-Design and the proposed Facility Safeguardability Analysis to go beyond the stage of discussion. More is said about the recommended path forward for Safeguards-by-Design, and enhancing engagement with the IAEA and the nuclear industry in this area in Reference 4.

Ultimately, the implementation of Safeguards-by-Design and systematic review of the Facility Safeguardability Analysis for proposed facilities, by respective groups at the IAEA, may require changes in the way the IAEA currently engages with the owner/operator building new nuclear facilities. It is envisioned that earlier engagement of the IAEA, especially regarding the analysis of the facility safeguardability, and review of the safeguards approach proposed by the designer, will ultimately strengthen the role of the IAEA in ensuring that new and more complex nuclear facilities can be adequately safeguarded.

# 9. PROSPECTIVE CASES FOR DEMONSTRATING FSA

Practical cases where Facility Safeguardability Analysis could be demonstrated include the following:

- Comparing and evaluating the safeguardability of the prismatic fuel vs. pebble fuel High Temperature Gas Reactor (Gen-IV NGNP)
- Comparing and evaluating safeguards measures for optimizing the safeguards verification of $UF_6$ process flows in a large enrichment plant (i.e. $UF_6$ cylinder portal monitor and load cell monitoring vs. on-line mass and enrichment flow monitoring of the enrichment header piping).
- Comparing and evaluating safeguards measures and approaches for pyroprocessing (i.e. pyrometallurgical reprocessing of spent nuclear fuel).

Enough design information exists in all three cases to permit an effective and conclusive test for Facility Safeguardability Analysis.

# 10. SUMMARY AND CONCLUSIONS

The authors have proposed and outlined the use of Facility Safeguardability Analysis (FSA) to: i) compare and evaluate nuclear safeguards measures, ii) optimize the proposed facility safeguards approach, iii) objectively and analytically evaluate nuclear facility safeguardability, and iv) evaluate and optimize barriers within the facility and process design to minimize the risk of the diversion of nuclear material. As envisioned, Facility Safeguardability Analysis would be used by the facility designer and/or Project Design Team during the design and construction of the nuclear facility to evaluate and optimize the proposed facility safeguards approach and design of the safeguards system. Through a process of “Safeguards-by-Design” (SBD), this would be done at the earliest stages of project conceptual design and would involve domestic and international nuclear regulators and authorities, including the International Atomic Energy Agency (IAEA). The benefits of the Safeguards-by-Design approach is that it would clarify at a very early stage the international and domestic safeguards requirements for the Project Design Team, and the best design and operating practices for meeting these requirements. It would also minimize the risk to the construction project, in terms of cost overruns or delays, which might otherwise occur if the nuclear safeguards measures are not incorporated into the facility design at an early stage. Incorporating nuclear safeguards measures is straight forward for nuclear facilities of established design, but becomes more challenging with facilities of radically new design and larger and more complex facilities. For this reason, the facility designer and project design team require an analytical method for comparing safeguards measures, options, approaches, and for evaluating the "safeguardability" of the facility.

This report explained how diversion path analyses, used in support of GIF and INPRO, could be adapted for evaluating and assessing the safeguardability of nuclear facilities – both existing, as well as those still on the drawing board. The advantages of the Facility Safeguardability Analysis is that it would give the facility designer an analytical tool for not only evaluating and assessing the safeguards measures and approaches for the prospective facility, but also the ability to optimize the design of the facility process for enhanced safeguardability. The report explained the need for Facility Safeguardability Analysis, proposed an approach for performing the analysis, and explained how Facility Safeguardability Analysis could be used in the context of the Safeguards-by-Design, in support of the design and construction of nuclear facilities.

The subject study and report were funded by the U.S. DOE National Nuclear Security Administration (NNSA) Office of NA-24, in support of the NNSA Next Generation Safeguards Initiative (NGSI), to improve the effectiveness and efficiency of international nuclear safeguards.

Based on the current need and potential gain from applying Facility Safeguardability Analysis, the authors recommend further developing Facility Safeguardability Analysis and demonstrating it on one or two concrete test cases to prove its utility. If the demonstration is successful, the authors further recommend presenting the Facility Safeguardability Analysis to the broader international nuclear safeguards community, the IAEA, and the nuclear industry to support the more systematic analysis and implementation of nuclear safeguards in new nuclear facilities under design and construction worldwide.

**In summary, the authors expect Facility Safeguardability Analysis (FSA) to:**

- Help define the functional requirements for the safeguards systems at the earliest design stage
- Ensure that the facility design will be amenable to international (IAEA) safeguards
- Provide assurance that the facility will be able to meet safeguards goals when completed
- Identify any potential technology gaps where the required performance is not attainable with current technologies, identify where new technologies are needed, or identify where change in the facility design is necessary
- Ensure that no surprises occur as the detailed design is developed
- Ensure that safeguards can be implemented effectively during all phases of plant operation (i.e., during startup, normal operation, maintenance shutdown, etc.)
- Identify opportunities for process or design modification to enhance safeguardability
- Provide a formalized structure for performing vulnerability analysis with expert elicitation in support of designing, evaluating, and developing the facility safeguards systems.

**In order to achieve these benefits, the following needs to be addressed to fully develop and standardize Facility Safeguardability Analysis:**

- Further develop the preliminary diversion path analysis to more clearly identify nuclear safeguards vulnerabilities in nuclear facility design
- Further develop the risk identification process
- Map and standardize the expert elicitation and overall analytical process
- Develop a scheme and metric for quantifying the safeguardability of the facility and/or process
- Integrate the diverse analytical tools and analyses in a structured and integrated whole
- Develop the analytical process in a modular manner so that it can be used for analyzing simple as well as very complex nuclear facilities

- Simplify the analytical process so that it can be used more easily by nuclear facility designers and Project Design Teams
- Demonstrate Facility Safeguardability Analysis, using a concrete test case to determine its effectiveness, ease of use, and possible short comings.

Some of the points above have been addressed to some degree in previous projects, in particular the preliminary diversion path analysis, as previously utilized in the Proliferation Risk Reduction Analysis (PRRA) projects sponsored by NNSA. However, the analytical tools need to adapted, simplified, and integrated for the designer to compare and evaluate specific safeguards measures and approaches for a new facility, and compare and evaluate process and safeguards system design options. This is what would be necessary for Facility Safeguardability Analysis to become viable.

**The cost and schedule to develop Facility Safeguardability Analysis is reduced because many of the required elements have previously been developed and demonstrated -** although they have not yet been integrated, nor fully adapted for use in the design process.

# 11. REFERENCES


1. International Atomic Energy Agency: *The Structure and Content of Agreements between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons*, INFCIRC/153 (Corrected), Para. 28, Vienna, Austria, June, 1972.

2. Stein, M, et al.: *Safety, Security, and Safeguards by Design – An Industrial Approach*, Proceedings of Global 2009, Paris, France, Sept. 6 – 11, 2009.

3. Whitlock, J., of Atomic Energy of Canada Limited (AECL): *Incorporating Proliferation Resistance in Reactor Design*, Presentation to the Institute of Nuclear Materials Management (INMM) Workshop for Users of Proliferation Assessment Tools, Texas A&M University, February 23-25, 2010.

4. Bjornard, T., et al.: *Implementing Safeguards-by-Design*, U.S. DOE Idaho National Laboratory report INL-EXT-09-17085, Idaho Falls, ID, February, 2010.

5. U.S. DOE National Nuclear Security Administration (NNSA): *Next Generation Safeguards Initiative*, NNSA Office of Nonproliferation and International Security (NA-24), Washington, D.C., January, 2008.

6. International Atomic Energy Agency: *IAEA Safeguards Glossary – 2001 Edition*, Para. 3.14, 3.15, and 3.20, Vienna, Austria, 2002.

7. Bjornard, T., et al.: *Institutionalizing Safeguards-by-Design*: *High-Level Framework*, Vol. 1, U.S. DOE Idaho National Laboratory report INL/EXT-08-14777, Rev. 1, Idaho Falls, Idaho, February, 2009.

8. International Atomic Energy Agency, Department of Safeguards: *Safeguards Manual - Part SMC, Safeguards Criteria*, Vienna, Austria, October, 2003. (IAEA Internal Document)

9. Boyer, B., et al.: *Safeguards-by-Design General Guidance*, U.S. DOE Los Alamos National Laboratory, Report LA-UR-09-05802, Los Alamos, New Mexico, September, 2009.

10. Durst, P. C., et al.: *Safeguards Guidance Document for Designers of Nuclear Facilities: International Nuclear Safeguards Requirements and Practices for High Temperature Gas Reactors (Prismatic Fuel HTGRs)*, U.S. DOE Idaho National Laboratory report INL-EXT-10-17981, April, 2010.

11. Durst, P. C., et al.: *Safeguards Guidance Document for Designers of Nuclear Facilities: International Nuclear Safeguards Requirements and Practices for High Temperature Gas Reactors (Pebble Fuel HTGRs)*, U.S. DOE Idaho National Laboratory report INL-EXT-10-18438, April, 2010.

12. Bari, R., et al.: *Proliferation Resistance and Physical Protection Evaluation Methodology Development and Applications*, U.S. DOE Brookhaven National Laboratory presentation to the GIF Symposium, BNL-90259-2009-CP, Paris, France, September 9 – 10, 2009.

13. International Atomic Energy Agency: *Design Measures to Facilitate Implementation of Safeguards at Future Water Cooled Nuclear Power Plants*, Technical Report Series No. 392, Vienna, Austria, 1998.

14. International Atomic Energy Agency: *International Target Values 2000 for Measurement Uncertainties in Safeguarding Nuclear Materials*, IAEA Report STR-327, Vienna, Austria, 2000.

15. Whitlock, J. (Atomic Energy of Canada Ltd.): Personal communication, ca. March, 2010.

16. International Atomic Energy Agency: IAEA Department Organization Chart, Vienna, Austria, March, 2009.