SAND2013-4023C

Security-by-Design Handbook

M. K. Snell[a], C. D. Jaeger[a], S. E. Jordan[a], C. Scharmer[a], K. Tanuma[b], K. Ochiai[b], T. Iida[b]

[a]Sandia National Laboratories, Albuquerque, New Mexico, USA

[b]Japan Atomic Energy Agency, Tokai-mura, Ibaraki, Japan

Abstract. This paper will provide an overview of a preliminary draft of a Security-by-Design (SeBD) Handbook [1] developed as part of collaboration between the Japan Atomic Energy Agency, Department of Science and Technology for Nuclear Material Management and Sandia National Laboratories. While there has been a significant amount of prior work on Safeguards by Design and work relevant to Safety by Design, there has been comparatively less documented on Security by Design. This preliminary draft of the Handbook is meant to be a first step to remedy this. The paper describes the SeBD Handbook which is divided into sections and includes a discussion of areas such as: basic definition of SeBD and why it is important, an approach or strategy for implementing SeBD, a set of physical protection principles and practices to assist in the implementation of the SeBD strategy and other useful details on how the principles and practices have been and can be applied.

1. Introduction

In recent years, there has been increasing attention worldwide on physical protection to prevent unauthorized removal of nuclear material and other radioactive materials and protection against sabotage. This has led to the release of several nuclear security documents by the International Atomic Energy Agency, most notably Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2]. This publication recommends significant changes in how physical protection is provided and calls for capabilities to locate and recover missing nuclear material and efforts to mitigate the effects of sabotage. At the same time as these documents have been released, a number of countries have begun programs to construct and build their first nuclear power plants (NPP) while other countries may develop nuclear fuel cycle facilities in the future. Thus, there is value in providing these countries guidance on efficiently and effectively providing physical protection for these against theft of nuclear material or sabotage.

The materials for the Security by Design (SeBD) Handbook were produced primarily as part of a bilateral project between the Japan Atomic Energy Agency (JAEA) Department of Science and Technology for Nuclear Material Management and Sandia National Laboratories (SNL), which represented the US Department Energy (DOE) National Nuclear Security Administration (NNSA). This Handbook is designed to introduce and describe what is called Security by Design, a framework designed to effectively and efficiently provide physical protection for nuclear materials and facilities over their lifetimes. This framework describes an approach for addressing the recommendations found in INFCIRC/225/Revision 5, within the context of developing a nuclear power plant or nuclear facility (NF).

For the purposes of the Handbook, SeBD will be described as the *system level* incorporation of physical protection features into a new nuclear power plant or nuclear facility, resulting in a Physical Protection System (PPS) design that minimizes, as much as possible, the risk of malicious acts leading to nuclear material theft; nuclear material sabotage, and facility sabotage, through features inherent in (or intrinsic to) the design of the facility. It can be viewed as a framework to achieve a robust, durable, and responsive security system.

2. Objective and Scope of the Handbook

The intent of this Handbook is to describe an approach for SeBD, starting with a strategy for achieving SeBD, and then show how that strategy can be implemented. This approach will be

explained within the framework of milestones in the development of a country's national nuclear infrastructure as described within what we will refer to as the Milestones documents [3, 4] and will address the objectives and fundamental principles found in Nuclear Security Series No. 13

The scope of this Handbook is to familiarize the reader with SeBD, to provide some insight on how to implement and achieve SeBD, and to cover principles and best practices that support this implementation. Emphasis is on integrating these physical protection principles and practices into different steps in the design process for the facility as well as the overall lifecycle of the facility. This document is aimed at decision makers, advisers, and senior managers in the governmental organizations, utilities, industries, and regulatory bodies of a country interested in developing nuclear power. Thus, there is a basic focus on defining and providing an overview of SeBD and how it can best be achieved.

3. Structure of the Handbook

The Handbook covers the following topics:

- An overview of the SeBD framework that discusses the value of using that framework in the design process;
- A description of a strategy for implementing SeBD within the context of the recommendations found in INFCIRC/225/Revision 5 and the Milestones documents;
- A detailed description of principles and best practices for achieving SeBD;
- A detailed discussion of how the application of SeBD principles and practices, to include how they can be and have been usefully implemented at both the competent authority and at the facility level;

Additional information on SeBD is organized into appendices that provide more detail on such topics as the SeBD design process and on principles and practices that merit more detailed discussion.

4. Security-by-Design Framework

The Handbook provides the context for SeBD by defining it, describing the value of following SeBD, and finally, several areas or factors, such as international security recommendations, engineering/regulatory principles and practices which contribute to SeBD.

4.1. What is SeBD

SeBD is the system level incorporation of the Physical Protection System (PPS) into a new nuclear power plant or nuclear facility resulting in PPS design that minimizes as much as possible the risk of malicious acts leading to nuclear material theft, nuclear material sabotage, and facility sabotage through features inherent in (or intrinsic to) the design of the facility. The intent of SeBD is that the design of a nuclear facility provides an adequate level of security throughout the lifetime of that facility in a way that is cost-effective and does not have negative impacts on operations, safety, and safeguards. The implication of this idea is that a facility should be designed to remain, as much as possible, secure over several decades of operation taking into account that unknown conditions and occurrences affecting security must be accounted for starting at the design phase.

4.2. What is the value of following SeBD

SeBD offers a systematic approach to addressing the following issues that have been experienced in the past:

- Late involvement of security in the design process that either led to less security or required expensive redesign and construction costs.
- PPS designs created with either no consideration of the threat or based only on consideration of the current threat.
- Lack of proper integration between security and operations, safety, and safeguards, leading to inefficiencies.

- Weaknesses in governance and organizational structures, especially concerning the competent authority and licensees.
- Little or no consideration of the facility lifecycle.

All of these factors have resulted in higher costs to develop and upgrade physical protection systems to meet the changing threat and have limited the potential for such systems to evolve over time. Implementation of SeBD is intended to provide design features that enable the PPS to remain effective and easier to upgrade when addressing the changing threat environment. This Handbook also covers a number of helpful design best practices that have been identified over the last 40-50 years to cut construction costs and increase the effectiveness and efficiency of the PPS for future plants.

4.3. Factors contributing to SeBD

In addition to design and construction stages that focus on the physical facility itself, there are other important considerations. Figure 1 represents some of the factors contributing to SeBD.

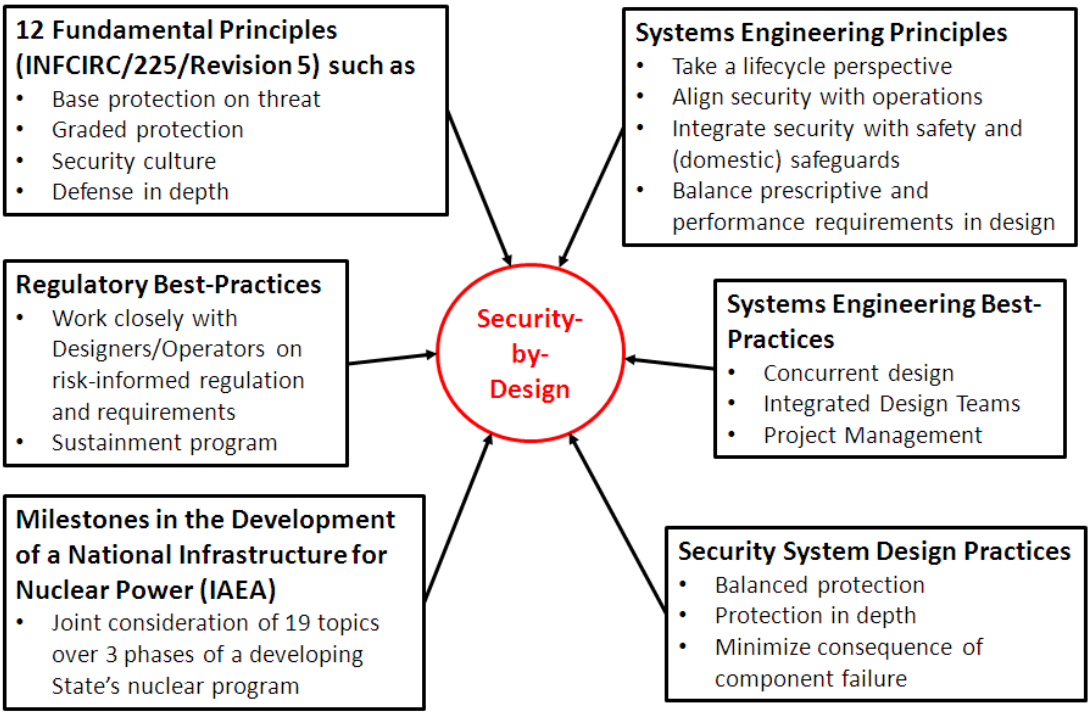

FIG. 1. Contributing Factors to SeBD

5. Strategy for Achieving Security-by-Design

In this section of the Handbook the basic strategy for achieving SeBD is discussed. Four main elements are described in more detail in the Handbook:

- **Integrated Design Team**: Incorporation of a physical protection team (PPT) within the context of the overall design team;
- **Risk Informed Design**: Use of a risk-informed design to decision-making process that addresses threat, vulnerability, and consequence;
- **Facility Design/Operations Lifecycle**: Use of a structured lifecycle process for the integrated design team, where details are provided for the activities that the PPT needs in order to achieve SeBD; and

- **Principles and Practices**: Discussion of a set of physical protection principles and practices, how these practices can be implemented, and a description of how these principles and practices can be integrated into the lifecycle process.

5.1. Integrated Design Team

The Integrated Design Team is composed of a set of cross-functional teams (each covering a different function, such as safety, security, and operations) that collectively performs the design and construction portion of the NPP or NF lifecycle. The integrated design team (shown schematically in Figure 2) works for the lead designer, and all teams are treated as having the same level of responsibility (although in particular areas there may be priorities set between the different teams).

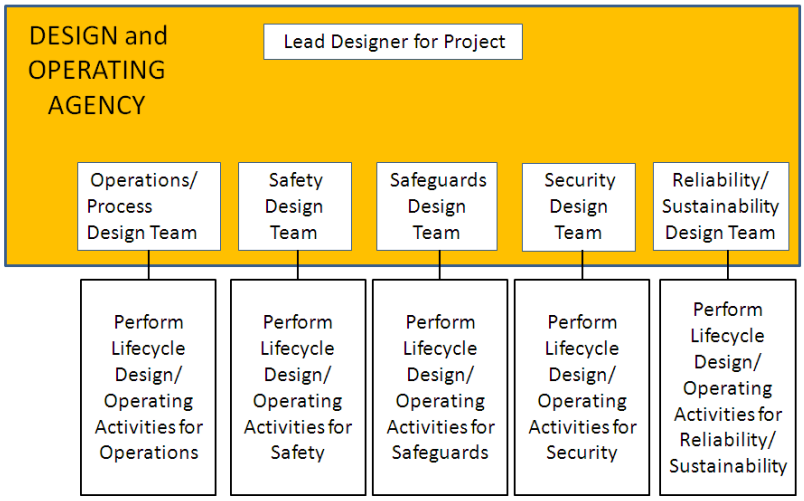

FIG. 2. Integrated Design Team

The use of this team approach has been shown to both reduce design time and to improve the effectiveness of the resulting system in performing each of the functional areas. Note that a similar figure can be constructed for the operational phase of the lifecycle, where these groups support the plant manager.

5.2. Risk-Informed Design

The use of risk-informed design has several important benefits that led to its inclusion as the second element of the strategy to achieve SeBD. Risk management is a central consideration in the lifecycle, whether the risk is due to project risk, safety, security, or safeguards risk. The term “risk informed” refers to decision-making processes that include risk as one of several metrics considered in making the decision(s); this compares to “risk based” decisions where risk is the primary factor driving the decision process. The Handbook has more detailed description of the risk-informed design to decision-making process, and addresses threat, vulnerability, and consequence. The process has two major components:

- The process for design and evaluation of the physical protection system within the context of a facility design.
- A risk-informed approach to analyzing the design against competent authority requirements based on the risk components: threat, vulnerability, and consequences.

The high-level steps of the design and evaluation process (DEPO) are shown in Figure 3. The analysis of the PPS design needs to assess the effectiveness of the PPS in terms of Probability of System Effectiveness, or P_E, as well as the effectiveness of the nuclear security features at the site,

including emergency response plans and contingency plans, to mitigate a sabotage attack or to recapture/recover nuclear material that has left the site.

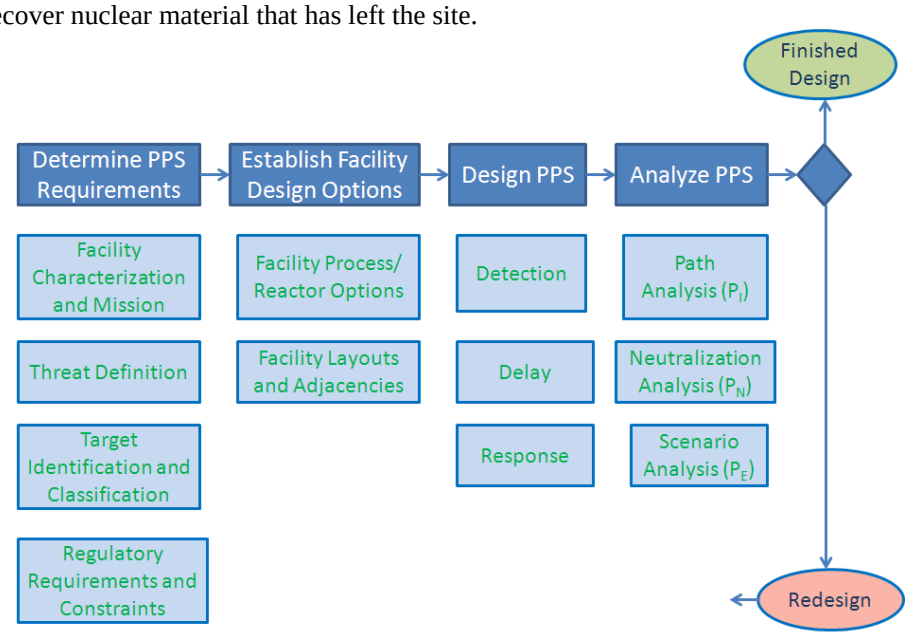

FIG. 3. Design and Evaluation Process

5.3. Facility Design/Operations Lifecycle

The third important element of the SeBD strategy is a focus on the lifecycle of the facility, especially during the design phase. Not only does the integrated design team need to consider the security requirements across the lifecycle of the facility, they need to have a good understanding of where different aspects of SeBD are best applied within the different phases of the lifecycle. Within the Handbook this section provides a detailed description of how the facility goes through various phases making up the facility lifecycle, from pre-conceptual planning to design, construction, operations, and dismantlement. It shows how the actions of the three entities (State, Design and Operating Agency, and PPT) can achieve SeBD. For the purposes of the Handbook, the facility lifecycle may be described as consisting of the following phases:

- **Project Scope and Planning Phase** includes all activities that commence before the particular Nuclear Facility (NF) project is approved.
- **Design Concept Phase** starts by defining facility mission needs statement and the lifecycle requirements for the facility, which includes the project team's assessment of the gap between desired and existing capability, the scope of the need, and associated potential hazards.
- **Design Engineering Phase** typically results in a PPS design with sufficient detail to support construction, plan development (such as response plans, emergency and contingency plans, and training plans), and development of a concept of operations.
- **Contracting Phase** assumes that an Architecture and Engineering (A&E) firm was selected to develop the design after project approval , while a separate construction firm is being contracted during this phase to perform the actual construction.
- **Construction Phase** is the phase in which the facility is built, and the site goes through formal acceptance procedures.
- **Fitness-to Operate-Phase** is the phase in which the competent authority conducts a “Fitness to Operate” evaluation.
- **Plant Operations Phase** is the phase where the facility operates normally until a decision is reached to cease operations.

- **Decommission and Dismantlement Phase** is the phase where decisions may be reached to remove any remaining nuclear material inventory and decisions are reached as to how to dismantle the facility.

Figure 4 shows the structure and depicts the lifecycle for facility design and operations, as the facility proceeds from pre-conceptual planning to design, construction, operations, and dismantlement (annotations in red font show activities specific to the PPT).

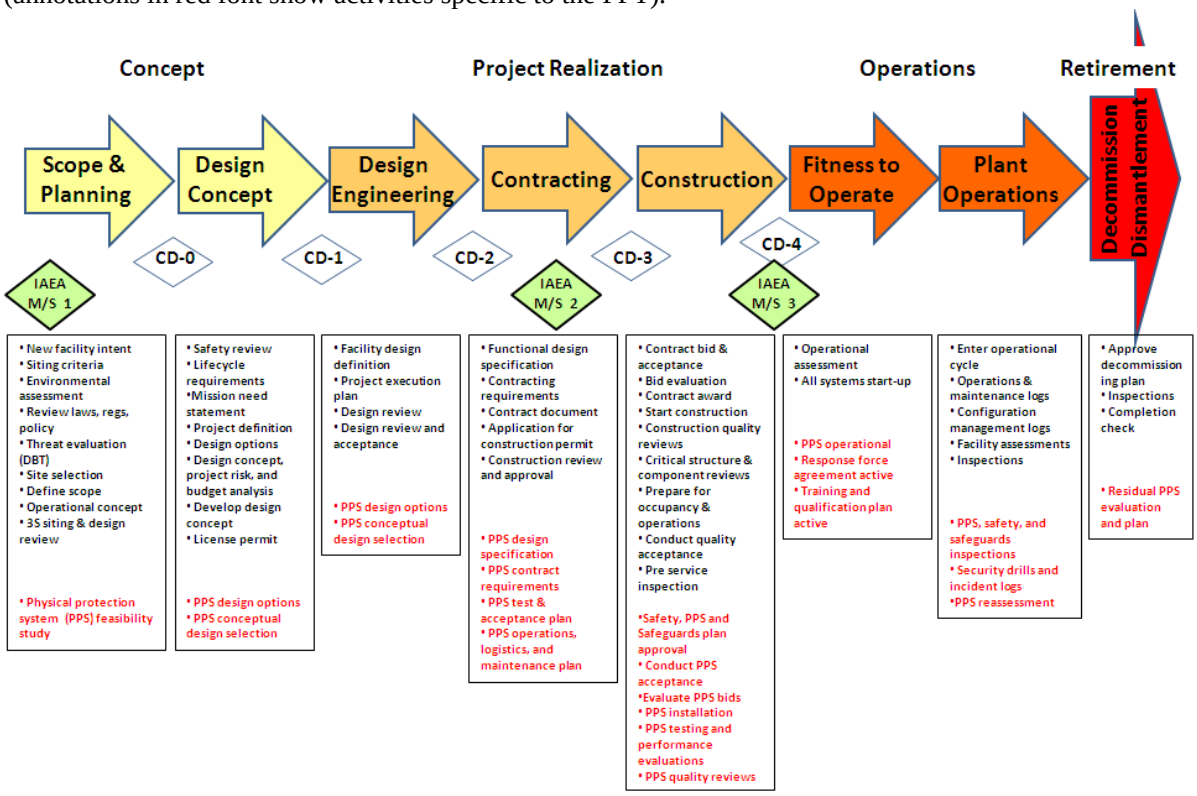

FIG. 4. Facility Design/Operations Lifecycle with Focus on the Security Dimension

5.4. Application of SeBD Principles and Practices

The fourth element of the SeBD strategy describes the principles and practices of the SeBD and is discussed in considerable detail within the Handbook.

6. Security-by-Design Principles and Practices

This Handbook also describes a set of SeBD principles and their associated best practices. The list of principles includes the 12 Fundamental Principles (A-L) of Physical Protection of Nuclear Material and Nuclear Facilities found in INFCIRC/225/Revision 5, so that the Handbook describes best practices that support each of the 12 Fundamental Principles. The Principles identified in the Handbook describe the "what." The Practices, the "how," provide information such as processes, methods, or technologies to meet the set of principles. For each fundamental principle, the principle is described first, associated practices are then described and explained, and the discussion for each principle ends with a table of the lifecycle phases where that principle and its practices can be applied. Shown in Figure 5 is an example table for Fundamental Principle A from INFCIRC/225/Revision 5.

	Lifecycle Phases								
Management Principles and Associated Practices	**Assumptions**	**Scope and Planning**	**Design Concept**	**Design Engineering**	**Contracting**	**Construction**	**License to Operate**	**Operational Phase**	**Decommissioning/ Dismantlement**
FUNDAMENTAL PRINCIPLE A: ***Responsibility of the State:*** The responsibility for the establishment, implementation and maintenance of a physical protection regime within a State rests entirely with that State.	Regime in place before Scope and Planning	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

FIG. 5. Management Principles and Lifecycle Phases

The Handbook also discusses best-practices associated with eight other principles that are more technical and are associated with design processes, systems engineering approaches, and project-management:

- **Inherent or intrinsic security** where physical protection is considered as part of siting and design of the facility layout and as opposed to after the facility design is almost completed.
- **Proven engineering principles** are used to design, build, operate and decommission nuclear facilities, to include use of proven approaches and adoption of commonly accepted guides and standards.
- **Proven project management principles** are used to design and build nuclear facilities to include explicit consideration of where interaction with competent authorities is needed and planning to allow time for critical decision-making.
- **Proven operational planning principles** are used to operate and decommission nuclear facilities to ensure that adequate security resources and trained security personnel are available.
- **Systems engineering principles** are used to design and build nuclear facilities, based on evaluation of commonly accepted systems engineering approaches [5].
- **Lifecycle perspective** is considered in the PPS design and operation to include both consideration of potentially increased threats over the life of the facility and of extra capacity in the design to accommodate future changes in the facility or physical protection technology.
- **Concept of operations** perspectives should be considered, to include coverage of normal, emergency, and security contingency conditions.
- **Synergy** between safety, safeguards and security should be considered and properly integrated across the lifecycle. Aspects to consider include requirements analysis, to include use of trade-off studies to determine conflicting requirements, looking for synergies between these functional areas, and using guides and standards to aid in integrating these functions.
- **Design in sustainability** where requirements to maintain, test, repair and upgrade the PPS are considered, to include the use of formal sustainability plans.
- **Balance** between prescriptive and performance requirements in the design should be considered, based on a good working relationship with the competent authority.
- **Validate effective communication** and/or agreements with other agencies, particularly emergency and security response organizations.
- **Project and operations experiences** in the form of lessons learned should also be considered.

6.1. Application of Principles and Practices

The Handbook includes a discussion of how the foregoing principles and practices can be applied. Practices described include those that competent authorities can take to encourage the application of SeBD, and others that designers can take to help implement SeBD at the facility layout level. It also discusses how adversary capabilities might change in the future and specific countermeasures that designers may be able to employ now to be ready for those changes.

6.2. Additional information on SeBD

The Handbook contains a number of appendices which provide additional information covering such topics as:

- **The Security by Design Generic Design Process,** describing the useful actions to achieve Security-by-Design by the three key entities: State, Design and Operating Agency, and Physical Protection Team over the facility lifecycle.
- **Diagrams Depicting the Relationship of Lifecycle Phases and Certain Project and Security Activities,** to include decision points and data flows.
- **More Information on Certain of the Principles and Practices**. More information is provided concerning some of the principles and practices and the discussion is grouped into six topical areas: Management Principles, Physical Protection Principles, General Technical Principles, General Human Element Principles, Systems Engineering Principles, and Other Specific Principles.

7. Summary

The intent of SeBD is that a nuclear facility be designed so that an adequate level of security can be provided throughout the entire lifetime of that facility, from construction through dismantlement/decommissioning, in a way that is cost-effective, addresses the evolving threat, and does not have negative impacts on operations, safety, and safeguards. SeBD is best achieved through a structured approach by which a State's nuclear security objectives are fully integrated throughout the life of the project, starting with project planning and scoping, and specifically integrated throughout the entire design and construction process of the facility.

This paper provides an overview of the Security by Design (SeBD) Handbook. It includes a discussion of some principles and practices, as well as practical insights on how to implement and achieve SeBD. The approach to SeBD is explained within the context of the framework of milestones in the development of a national nuclear infrastructure and is aligned with the objectives and fundamental principles found in Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). The hope is that this Handbook will lead to an earlier introduction of these principles and practices into the facility design process for new or existing nuclear power plants and facilities, resulting in more efficient and effective security.

REFERENCES

[1] SANDIA NATIONAL LABORATORIES, SAND 2013-0038, *Security-by-Design Handbook,* Jan 2013.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Revision 5), Nuclear Security Series No. 13, Vienna, 2011.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, *Milestones in the Development of a National Infrastructure for Nuclear Power*, Nuclear Energy Series, No. NG-G-3.1, Vienna, 2007.

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, *Evaluation of the Status of National Nuclear Infrastructure Development*, Nuclear Energy Series, No. NG-T-3.2, Vienna, 2008.

[5] INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING (INCOSE), *Systems Engineering Handbook,* Version 3.2, 2010