

SANDIA REPORT

SAND2013-0038

Unlimited Release

Printed January 2013

Security-by-Design Handbook

Mark K. Snell, Calvin D. Jaeger, Sabina E. Jordan, and Carol Scharmer
Sandia National Laboratories, Albuquerque, New Mexico, USA

Koji Tanuma, Kazuya Ochiai, and Toru Iida
Japan Atomic Energy Agency, Tokai-mura, Ibaraki, Japan

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.



Japan Atomic Energy Agency



Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: <http://www.osti.gov/bridge>

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: <http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online>



SAND2012-0038
Unlimited Release
Printed January 2013

Security by Design Handbook

Mark K. Snell, Calvin D. Jaeger, and Carol Scharmer
International Physical Security
Sabina E. Jordan
Policy and Decision Analytics
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS6833

Koji Tanuma, Kazuya Ochiai, and Toru Iida,
Japan Atomic Energy Agency, Tokai-mura, Ibaraki, Japan

Abstract

This document is a draft Security-by-Design (SeBD) handbook produced to support the Work Plan of the Nuclear Security Summit to share best practices for nuclear security in new facility design. The Work Plan calls on States to “encourage nuclear operators and architect/engineering firms to take into account and incorporate, where appropriate, effective measures of physical protection and security culture into the planning, construction, and operation of civilian nuclear facilities and provide technical assistance, upon request, to other States in doing so.”

The materials for this document were generated primarily as part of a bilateral project to produce a SeBD handbook as a collaboration between the Japan Atomic Energy Agency (JAEA) Nuclear Nonproliferation Science and Technology Center and Sandia National Laboratories (SNL), which represented the US Department Energy (DOE) National Nuclear Security Administration (NNSA) under a Project Action Sheet PAS-PP04. Input was also derived based on tours of the Savannah River Site (SRS) and Japan Nuclear Fuel Limited (JNFL) Rokkasho Mixed Oxide Fuel fabrication facilities and associated project lessons-learned.

For the purposes of the handbook, SeBD will be described as the system-level incorporation of the physical protection system (PPS) into a new nuclear power plant or nuclear facility resulting in a PPS design that minimizes the risk of malicious acts leading to nuclear material theft; nuclear material sabotage; and facility sabotage as much as possible through features inherent in (or intrinsic to) the design of the facility. A four-element strategy is presented to achieve a robust, durable, and responsive security system.

ACKNOWLEDGMENTS

The authors would like to thank Janette Hill of NNSA and Jose Rodriguez and David Olson, both formerly from Sandia National Laboratories, for starting the Security by Design project on the US side and their early work in this area. A note of thanks is also due to Rudy Matalucci, formerly from Sandia National Laboratories, for his insights into how security engineering and risk assessment contribute to Security by Design.

Table of Contents

Executive Summary	13
1 Introduction.....	16
1.1 Background	16
1.2 Objective of this Document	17
1.3 Scope	17
1.4 Users	17
1.5 Structure.....	18
2 Security-by-Design	20
What Is the Value of Following Security-by-Design?	21
Factors Contributing to Security-by-Design	22
2.1 Context for SeBD within the Milestones Documents and the INPRO Assessment Methodology	23
2.2 Assumptions.....	25
3 Strategy for Achieving Security-by-Design	26
3.1 Integrated Design Team.....	26
3.2 Risk-Informed Design.....	28
3.3 Facility Design/Operations Lifecycle	32
4 SeBD Principles and Practices	44
4.1 Fundamental Principle A— <i>Responsibility of the State</i>	45
4.2 Fundamental Principle B— <i>Responsibilities during International Transport</i>	46
4.3 Fundamental Principle C— <i>Legislative and Regulatory Framework</i>	47
4.4 Fundamental Principle D— <i>Competent Authority (CA)</i>	49
4.5 Fundamental Principle E— <i>Responsibility of the License Holders</i>	50
4.6 Fundamental Principle F— <i>Security Culture</i>	52
4.7 Fundamental Principle G— <i>Threat</i>	54
4.8 Fundamental Principle H— <i>Graded Approach</i>	56
4.9 Fundamental Principle I— <i>Defense in Depth</i>	58
4.10 Fundamental Principle J— <i>Quality Assurance</i>	61
4.11 Fundamental Principle K— <i>Contingency Plans</i>	63
4.12 Fundamental Principle L— <i>Confidentiality</i>	65
4.13 Other SeBD Principle— <i>Achieve Inherent or Intrinsic Security</i>	66
4.14 Other SeBD Principle— <i>Proven Engineering Principles</i>	68
4.15 Other SeBD Principle— <i>Proven Project Management Principles</i>	69

4.16	Other SeBD Principle— <i>Proven Operational Planning Principles</i>	71
4.17	Other SeBD Principle— <i>Systems Engineering Principles</i>	74
4.18	Other SeBD Principle— <i>Lifecycle Perspective</i>	76
4.19	Other SeBD Principle— <i>Concept of Operations Perspective</i>	78
4.20	Other SeBD Principle— <i>Synergy between Safety, Safeguards, and Security</i>	80
4.21	Other SeBD Principle— <i>Design-in Sustainability</i>	82
4.22	Other SeBD Principle— <i>Balance Prescriptive and Performance-Based Requirements</i>	84
4.23	Other SeBD Principle— <i>Validate Effective Communication and/or Operational Agreements with Other Agencies</i>	85
4.24	Other SeBD Principle— <i>Project and Operations Experience</i>	86
5	Detailed Application of the Principles and Practices	88
5.1	Competent Authority Practices That Support SeBD	88
5.2	Implementing Security by Design at the Facility Level.....	89
5.3	Possible Areas Where the DBT/TA Capability May Increase in the Future.....	92
6	Summary	94
	References.....	95
	Appendix A – Security by Design Generic Design Process.....	98
A.1	Scope and Planning Phase.....	98
A.2	Project Phase	99
A.3	Leading to CD-0, Project Authorization.....	100
	Scope and Planning (Project)	100
A.4	Leading to CD-1, Conceptual Design	101
	Concepts and Design Options	101
A.5	Leading to CD-2, Design Approval.....	102
	Design Engineering and Schematics	102
A.6	Leading to CD-3, Construction Approval	103
	Contract Definition and Contract Award	103
A.7	Leading to CD-4, Acceptance	104
A.8	Operational Phase	107
A.9	Decommissioning and Dismantlement Phase	110
	Appendix B - Evaluating Security Risk Assessment Factors.....	112
	Appendix C - Security Risk Management	114
	Appendix D – Relationship of Lifecycle Phases and Certain Project and Security Activities	116
	Appendix E – More Information on the Principles and Practices.....	120
E.1	Introduction.....	120
E.2	Topical Area: Management Principles	122

E.3	Topical Area: Physical Protection Principles.....	122
	Best Practices for Physical Protection	123
	Design Basis Threat and Threat Assessment	123
	Implementing a Graded Approach	127
	Target Categorization for Unauthorized Removal	128
	Vital Area Protection and Vital Equipment.....	130
	Use of the International Nuclear Event Scale	132
	Evaluating Consequences of Malevolent Acts.....	134
	Intrinsic Security.....	134
	Flexibility	137
E.4	Topical Area: System Engineering Principles.....	137
	View the PPS from a lifecycle perspective	137
	Synergy between Safety, Safeguards, and Security	137

List of Figures

Figure 1.	Physical Protection System Objective	20
Figure 2.	Contributing Factors to SeBD	22
Figure 3.	Integrated Design Team	27
Figure 4.	Design and Evaluation Process.....	29
Figure 5.	Facility Design/Operations Lifecycle.....	34
Figure 6.	Facility Design/Operations Lifecycle with Focus on the Security Dimension	34
Figure 7.	Japanese Implementing Procedure for Nuclear Power Plants.....	37
Figure 8.	Diagram of Notional Lifecycle	38
Figure 9.	Feasibility Study Logic Flow	40
Figure 10.	Design and Operations Activities for the Design Engineering Phase.....	41
Figure 11.	Defense in Depth Preventive and Protective Measures against Insiders.....	59
Figure 12.	ISO 15288:2008 Processes.....	74
Figure 13.	Target, Facility Design, and Response Analysis	91
Figure 14.	Layout versus Personnel/Material Flows and Security Areas	92
Figure 15.	Scope and Planning.....	100
Figure 16.	Conceptual Design	102
Figure 17.	Design Engineering	103
Figure 18.	Contracting.....	104
Figure 19.	Construction.....	106

Figure 20. Acceptance	107
Figure 21. Operational Phase	109
Figure 22. Decommissioning and Dismantlement	110
Figure 23. Security Risk Assessment Factors	112
Figure 24. Risk Assessment Management Alternatives	115
Figure 25. Activities during Scope, Planning, Project Definition, and Conceptual Design	116
Figure 26. Activities during Design Engineering and Contracting.....	117
Figure 27. Activities during Construction and Fitness to Operate (Transition to Operations)	118
Figure 28. Activities during Operations and Decommissioning/Dismantlement	119

List of Tables

Table 1. Interactions between the Five Integrated Design Team Functional Areas.....	27
Table 2. Lifecycle Phases and Associated Project Activities.....	36
Table 3. Assessments in Lifecycle	39
Table 4. Threat Capabilities That Might Change over Time and Possible Design Countermeasures	93
Table 5. Topical Groupings of the Fundamental Principles and Other SeBD Principles.....	121
Table 6. Outsider Threat Matrix	125
Table 7. INFCIRC/225/Rev 5 Table 1 Covering Nuclear Material Categories.....	129
Table 8. International Nuclear Event Scale.....	133

Acronyms

3S	Safety, Security, and Safeguards
A&E	Architecture and Engineering (firm)
BNI	Balance of Nuclear Island
BWR	Boiling water reactor
CD	Critical Decision
ConOps	Concept of Operations
DBT	Design Basis Threat
DEPO	Design and Evaluation Process Outline
DOE	Department of Energy
HPCI	High-Pressure Core Injection
IAEA	International Atomic Energy Agency
INL	Idaho National Laboratory
INPRO	International Project on Innovative Nuclear Reactors and Fuel Cycles
JAEA	Japan Atomic Energy Agency
LOCA	Loss of Coolant Accident
MC&A	Material Control and Accountability
METI/NISA	Ministry for Economy, Trade, and Industry/Nuclear and Industrial Safety Agency
M&O	Maintenance and Operations
NEPIO	Nuclear Energy Program Implementing Organization
NF	Nuclear Facility
NNSA	National Nuclear Security Agency
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
PEP	Project Execution Plan
PMBoK	Project Management Institute, <i>Project Manager Body of Knowledge</i> , (December 2008).
PP	Physical Protection
PPS	Physical Protection System
PPT	Physical Protection Team
PWR	Pressurized Water Reactor
SeBD	Security By Design
RAMs	Risk Assessment Methodologies
RCIC	Reactor Core Isolation Cooling
RCM	Reliability Centered Maintenance
SNM	Special Nuclear Material
SSNM	Strategic Special Nuclear Material
TA	Threat Analysis
USNRC	United States Nuclear Regulatory Commission

Definitions

Design and Operating Agency	Combined term for the agency responsible for the design, construction, and project acceptance of the completed facility before a Competent Authority inspection, as well as the agency or licensee responsible for the operation and maintenance of a Nuclear Power Plant or Nuclear Facility (NPP/NF). Alternatively, this collective term could be "owner." In practice, the design and operating agency can be two different agencies. The project team and management team are entities within this principal entity responsible for design, construction, and acceptance, and for operation and maintenance, respectively.
Nuclear Safeguards	Practices to assure that nuclear material and other specified items are not diverted from peaceful nuclear uses.
Nuclear Safety	The achievement of: <ul style="list-style-type: none">• proper operating conditions• prevention of <i>accidents</i>• mitigation of <i>accident</i> consequences, resulting in <i>protection of workers</i>• protection of the public and the environment from undue <i>radiation</i> hazard
Nuclear Security	The prevention and detection of, and response to: <ul style="list-style-type: none">• theft• sabotage,• unauthorized access, illegal transfer, or other <i>malicious</i> acts involving <i>nuclear material</i>, other <i>radioactive substances</i> or their associated <i>facilities</i>
Physical Protection Team (PPT)	<p>The PPT is an entity within the project team charged with the responsibility for the design, construction oversight, and acceptance of the completed PPS in conjunction with NPP/NF project activities performed before a Competent Authority inspection. During operations, the PPT is an entity within the Operating Agency's management team and refers to those responsible for the operation and maintenance of the PPS.</p> <p>The PPT assists the facility in understanding and developing the Protection Model or Theme that will be used at the facility. Therefore, the PPT should be considered one of the highly specialized teams that are an integral part of the overall project team and should include qualified security professionals with significant experience in design and evaluation of security designs and operations. With the new requirements for implementing security from performance-based requirements, the PPT should be identified as early as possible during the NPP/NF conceptual phase and should remain an integral part of the design team through the design and implementation phases.</p> <p>During the validation assessment, the PPT validates that the PPS system performance conforms to the defined concept of operations (ConOps),</p>

	Response Force Agreements, and the Training and Qualification program. All must be in place, fully implemented, and assure effective PPS operation.
Protection Model or Theme	The overall protection strategy for the facility or State, including the detection, delay, and response systems implemented at the facility. The protection theme is defined by: <ul style="list-style-type: none"> • PPS concept of operations • PPS system design • PPS personnel training and qualification plans • Response force and other security plans • Contingency plans
Safety, Safeguards and Security (3S)	Security must be in balance with safety and safeguards. The project team must reconcile all safety, safeguards, and security (3S) disciplines to ensure sufficiency in each.
Security Theme	Description of how security will be implemented, including defining limitations, such as who provides armed response. The security theme includes concept of operations and the protection model or strategy.
State	The inclusive term for all physical protection regime organizational elements, including legislative, executive, regulatory, and competent authority. The State may create a nuclear energy program implementing organization (NEPIO), which would be an entity within the State.

Executive Summary

All nuclear facilities must employ engineering and administrative controls to assure the safety, safeguards, and security of facilities and materials. The terms safety, safeguards, and security encompass the “protective” objectives of nuclear facilities. The principal objective of safety is to reduce or eliminate the risk from non-malicious random events resulting in injury, death, nuclear material dispersal, or property damage. The objective of safeguards is the timely detection of diversion of significant quantities of nuclear material by the State from peaceful nuclear activities to the manufacture of nuclear weapons or of other nuclear explosive devices and to detect undeclared nuclear material and activities in a State.” The objective of security is to minimize the risk of malicious acts resulting in nuclear material theft, nuclear material sabotage, and nuclear facility sabotage. Together, safety, safeguards, and security form the “3S” of nuclear material and facility management.

There is an increasing international awareness that an efficient and effective nuclear facility design is best achieved when requirements from the 3S disciplines—Safety, Safeguards, and Security—are balanced and intrinsic to the facility design. This can be achieved through an understanding of 3S policies, processes, methods, and technologies, and by applying them during all phases of the design process. These concepts are central to what might be viewed as a “X by design” approach to design where X is safety, safeguards, or security, or 3S itself. 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 (SeBD). This draft handbook is meant to be a first step to remedying this.

In order to be truly effective, Security by Design principles should be applied to a project from the conceptual stage forward. Since a nuclear facility may be operational for 60-80 years or more, possibilities for changes to the facility, due to changes in in the security threat or evolving security technology or changes in facility operations, should be considered in its design.

The primary audience for this handbook—decision makers, advisers and senior managers in the governmental organizations, utilities, industries, and regulatory bodies—are advised to focus on Section 2 for a basic understanding of SeBD and why it is important to achieving efficient and effective physical protection.

Section 3 describes an approach or strategy for implementing SeBD within the context of the recommendations found in Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) Nuclear Security Series No. 13. This section begins with a general description of the strategy for achieving SeBD, and then shows how that strategy can be implemented. Emphasis is on integrating physical protection principles and practices into different steps in the design process for the facility throughout the lifecycle of the facility (Appendix A describes a generic SeBD design process). Safety, safeguards, and security (3S) objectives are stressed during the entire design process, starting with pre-conceptual planning. The hope is that this handbook will lead to earlier introduction of these principles and practices into the

facility design process for new or existing nuclear power plants (NPPs) and nuclear facilities (NFs), resulting in more efficient and effective security.

The strategy for implementing SeBD includes the use of:

1. Integrated Design Team: Incorporation of a Physical Protection Team (PPT) within the context of the overall design team reporting to a Project Manager who has responsibility for implementing Safety, Security, Safeguards, Operations, and Sustainability/Reliability and is supported in carrying out that responsibility by the Project Leads in each of these areas;
2. Risk Informed Design: Use of a risk-informed design decision making process that addresses threat, vulnerability, and consequence;
3. Facility Design/Operations Life Cycle: Use of a structured lifecycle process for the integrated design team providing details about the activities that the PPT needs to perform to achieve SeBD from the earliest conceptual phases to facility dismantlement; and
4. Application of SeBD Principles and Practices: Application of a set of SeBD principles and practices that will yield more efficient and effective physical protection systems if integrated early into the facility lifecycle process.

Section 4 provides a set of physical protection principles and practices serving as the fourth component to assist in the implementation of the SeBD strategy. A number of principles and practices are presented and described along with a table showing what phases of the facility lifecycle each principle and practice can be applied. The physical protection principles and best practices to achieve SeBD found in section 4 were gathered from International, Japanese, and US sources. Principles are included for achieving security early in the design process where security requirements are typically less costly and easier to incorporate, and to avoid expensive retrofits and expansions. Required expansions might not be possible if a condition is not foreseen, and a new facility would be required.

Section 5 provides some useful details on how the principles and practices have been and can be applied. It includes, among other things, a discussion of lessons learned for SeBD at the competent authority and facility levels as well as some possible areas where the Design Basis Threat or Threat Assessment capabilities may increase in the future.

The materials for this document were produced primarily as part of a bilateral project to produce a SeBD handbook covering implementation of SeBD for nuclear power plants (NPPs) and nuclear facilities (NFs), as part of a collaboration between the Japan Atomic Energy Agency (JAEA) Nuclear Nonproliferation Science and Technology Center and Sandia National Laboratories (SNL), which represented the US Department Energy (DOE) National Nuclear Security Administration (NNSA). Input was also derived based on tours of the Savannah River Site and Japan Nuclear Fuel Limited Rokkasho Mixed Oxide Fuel fabrication facilities, and lessons-learned associated with these construction projects.

The production of this handbook is a step in the Japan-US Joint Nuclear Energy collaboration conducted under the Project Action Sheet PAS-PP04 between the United States Department of Energy and the Japan Atomic Energy Agency.

This handbook has been produced in part to support the Work Plan of the Nuclear Security Summit to share best practices for nuclear security in new facility design. The Work Plan calls on states to “encourage nuclear operators and architect/engineering firms to take into account and incorporate, where appropriate, effective measures of physical protection and security culture into the planning, construction, and operation of civilian nuclear facilities and provide technical assistance, upon request, to other States in doing so.”

1 Introduction

1.1 Background

In recent years, particularly after the September 11, 2001, attacks, there has been increasing attention worldwide on physical protection to prevent unauthorized removal of nuclear and 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) which calls for 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, a number of countries have begun programs to construct and build their first nuclear power plants while other countries may develop fuel cycle facilities in the future. Thus, there is value in providing these countries guidance on efficiently and effectively providing physical protection for these facilities and associated transport of nuclear material.

Finally, there has been a large body of experience over the last 30 years in developing physical protection systems (PPSs) based either on design basis threats (DBTs) or Threat Assessments (TA), as well as operating such facilities over time. This experience has led to a number of principles and practices for planning changes to facility PPSs as threats change over time.

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 facility.

Based on historic experience, security-by-design (hereafter designated as SeBD¹) is best implemented 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.

For the purposes of this handbook, SeBD will be described as the *system level* incorporation of the physical protection system into a new nuclear power plant or nuclear facility, resulting in a Physical Protection System 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.

¹ "SeBD" is used in this document to differentiate from Safeguards by design, often abbreviated as SBD.

It is important to note that the materials for this document were produced primarily as part of a bilateral project to generate a Security by Design (SeBD) handbook as a collaboration between the Japan Atomic Energy Agency (JAEA) Nuclear Nonproliferation Science and Technology Center and Sandia National Laboratories (SNL), which represented the US Department Energy (DOE) National Nuclear Security Administration (NNSA). Input was also derived based on tours of the Savannah River Site and Japan Nuclear Fuel Limited Rokkasho Mixed Oxide Fuel fabrication facilities and lessons-learned associated with these construction projects. The production of this preliminary draft is a step in the Japan-US Joint Nuclear Energy collaboration conducted under the Project Action Sheet PAS-PP04 between the United States Department of Energy and the Japan Atomic Energy Agency. As such, it culminates a series of activities to research and review design processes and to identify principles and practices that best describe and instruct implementation of security-by-design for nuclear power plants (NPPs) and nuclear facilities (NFs).

This volume has been produced to support the Work Plan of the Nuclear Security Summit to share best practices for nuclear security in new facility design. The Work Plan calls on States to “encourage nuclear operators and architect/engineering firms to take into account and incorporate, where appropriate, effective measures of physical protection and security culture into the planning, construction, and operation of civilian nuclear facilities and provide technical assistance, upon request, to other States in doing so.”

1.2 Objective of this Document

The intent of this handbook is to describe an approach to SeBD, starting with a strategy for achieving SeBD, and then showing how that strategy can be implemented. This approach will be explained within the the framework of milestones in the development of a national nuclear infrastructure as described within what we will refer to as the Milestones documents [1, 2] and will address the objectives and fundamental principles found in Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), reference [3].

1.3 Scope

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 practices that support this implementation.

1.4 Users

As is the case with the Milestones documents, 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.

Other organizations, such as donors, suppliers, nuclear energy agencies, and operator organizations may also use this publication to better understand their role in supporting security by design.

1.5 Structure

This handbook is structured to describe an approach to SeBD, starting with a strategy for achieving SeBD, and then showing how that strategy can be implemented. Emphasis is on integrating physical protection principles and practices into different steps in the design process for the facility as well as the overall lifecycle of the facility. Along the way, it will discuss how safety, safeguards, and security objectives can be jointly addressed during the entire design process, starting with pre-conceptual planning. The hope is that this handbook will lead to 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.

The handbook is divided into the following sections:

- Section 2 provides an overview of the SeBD framework and discusses the value of using that framework to develop NPPs and NFs;
- Section 3 describes an approach or strategy for implementing SeBD within the context of the recommendations found in INFCIRC/225/Revision 5 [3] and the Milestones documents [1,2];
- Section 4 describes Principles and Practices for achieving SeBD (note that this section can be omitted or skimmed by the reader on first review of this document);
- Section 5 describes in some detail on how the SeBD framework has been and can be applied.

The primary audience for this handbook—decision makers, advisers, and senior managers in the governmental organizations, utilities, industries, and regulatory bodies—are advised to focus on Section 2 for a basic understanding of SeBD and Section 5 for discussion of applications. Some understanding of Sections 3 and 4 is helpful but not required for those readers. Sections 3 and 4 provide more details into SeBD for readers interested in these specifics; these sections may also be useful for more technically inclined readers in the secondary audience to understand SeBD.

The approach to SeBD found in section 3, starts with a general description of strategy for achieving SeBD, and then shows how that strategy can be implemented. Emphasis is on integrating physical protection principles and practices into different steps in the design process for the facility throughout the lifecycle of the facility (Appendix A describes a generic SeBD design process). Safety, safeguards, and security (3S) objectives are stressed during the entire design process, starting with pre-conceptual planning. The hope is that this handbook will lead to earlier introduction of these principles and practices into the facility design process for new or existing nuclear power plants (NPPs) and nuclear facilities (NFs), resulting in more efficient and effective security.

The physical protection principles and best practices to achieve SeBD found in section 4 were gathered from International, Japanese, and US sources. Principles are included for achieving security early in the design process where security requirements are typically less costly and easier to incorporate, and avoid expensive retrofits and expansions. Required expansions might not be possible if a condition is not foreseen, and a new facility would be required.

The handbook includes all of the material found in earlier Task Reports produced as part of the collaborative project between JAEA and NNSA.

2 Security-by-Design

As described earlier, Security-by Design (SeBD)² 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 a nuclear facility be designed so that an adequate level of security can be provided 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 built in 2015 should be designed to remain, as much as possible, secure through 2075, taking into account that unknown conditions and occurrences affecting that facility in the future must be accounted for from the time of its design. Examples of unforeseen conditions might include the need for increased security at a facility due to changes in the security threat, in operations, or in evolving security technology that needs to be incorporated in the future, such as newer communications network or transmission technologies.

SeBD is best implemented 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.

The State's threat evaluation is the design basis for the PPS. The overarching objective of Security-by-Design is to allow mission achievement while security exceeds threat capability (Figure 1). Moreover, the NPP or NF needs to meet or exceed this threat capability throughout the operational lifetime of the plant and during dismantlement/decommissioning.

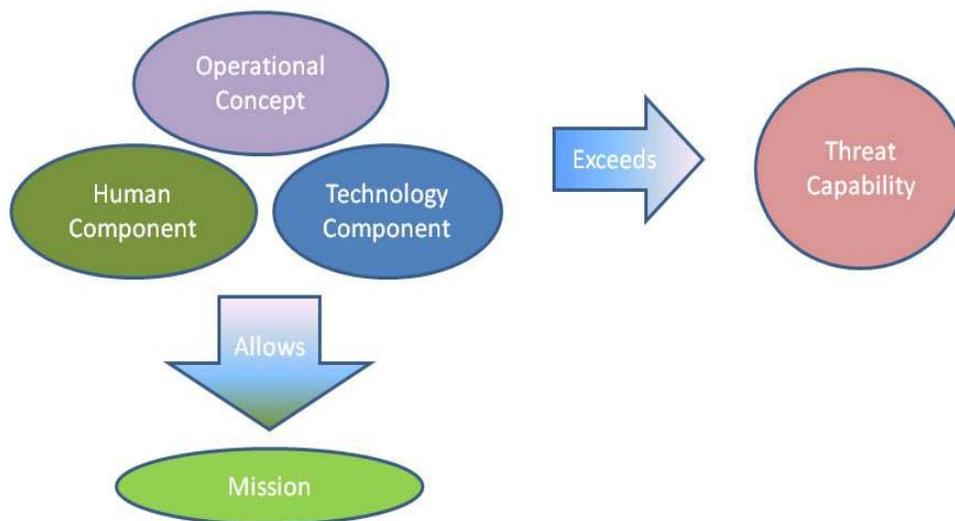


Figure 1. Physical Protection System Objective

² "SeBD" is used in this document to differentiate from Safeguards by design, often abbreviated as SBD.

What Is the Value of Following Security-by-Design?

Security-by-Design offers a systematic approach to addressing the following issues:

- Late involvement of security in the design process that either led to less security or required expensive redesign and construction costs. Historically, consideration of the PPS design in NPPs and NFs was delayed until a relatively late phase of plant/facility design, after many facility design details had been established and could not be changed to accommodate security.
- PPS designs created with either no consideration of the threat or based only on consideration of the current threat. As time progressed after construction, the threats to the NPP/NF have typically become more capable. As a result, licensees have been faced with the dilemma of making PPS improvements that are very expensive, have large negative operational impacts, or are not consistent with social norms in the host country; or having to accept a higher risk associated with newer, more capable threat attacks. For example, the following threats currently discussed in INFCIRC/225/Rev 5 [3] caused relatively little concern 25 years ago:
 - Cyber threats
 - Insider threats
 - Stand-off attacks
- Lack of proper integration between security and operations, safety, and safeguards, leading to inefficiencies. The conflicts between security and other important functions, such as operations, safety, and safeguards, were not anticipated early in the design phase, forcing uncomfortable trade-offs between requirements that were solved in ways that impacted the effectiveness of the PPS. At the same time, designers did not exploit possible ways in which security and other functions could be improved to benefit both security and the other function(s).
- Weaknesses in governance and organizational structures, especially concerning the competent authority and licensees. This would include stakeholders not communicating effectively to one another about how to improve security, leading to both increased costs and decreased security.
- Little or no consideration of the facility lifecycle. Security systems were developed to address the physical protection of the facility when it opened, within the context of either no Design Basis Threat/Threat Assessment (DBT/TA) or merely the current DBT/TA. This focus missed opportunities to take advantage of safety and safeguards features and the future requirements of the physical protection system and/or the DBT/TA.

All of these factors have resulted in higher costs to develop and upgrade physical protection systems to meet the changing threat and 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.

Factors Contributing to Security-by-Design

In addition to design and construction stages that focus on the physical facility itself, there are other important considerations. Equally important are a robust nuclear security culture and active quality and configuration management systems to support the PPS, and a periodic assessment of the PPS performance with respect to the current threat definition.

Implementation of SeBD practices is very important to having a cost effective and efficient protection system design for nuclear facilities. These practices include:

- Integration of all security design activities into the facility design/operation lifecycle
- Application of physical protection principles and best practices
- Consideration of integration of 3S into the design
- Risk management of potential impacts to the facility from a range of malevolent threats over the entire lifecycle of the nuclear facility, from concept to retirement
- Use of systems engineering best practices

Figure 2 represents some of the factors contributing to SeBD.

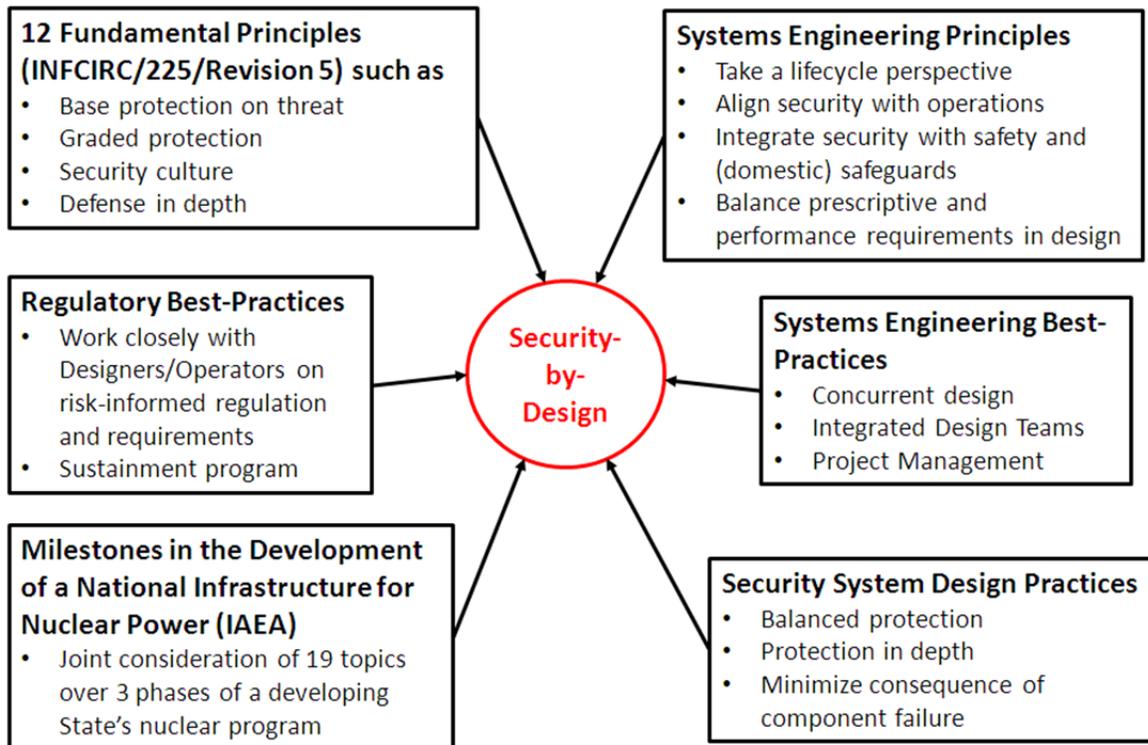


Figure 2. Contributing Factors to SeBD

2.1 Context for SeBD within the Milestones Documents and the INPRO Assessment Methodology

As mentioned earlier, the SeBD approach can be explained within the context of the framework of milestones in the development of a national nuclear infrastructure as described within what we refer to as the Milestones documents, references [1] and [2], as well as the assessment methodology documented by the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) in reference [4] for evaluating the use of an innovative nuclear energy system under a physical protection regime in a country that is planning to install a nuclear power program.

The Milestones documents cover the following topics related to SeBD:

- SeBD is applied within the legislative and regulatory framework of a physical protection regime. In turn, the establishment and implementation of a physical protection regime occurs as part of the process for developing the infrastructure necessary to support a nuclear power program.
- The 18 other infrastructure issues addressed (in addition to security), can have supportive (or synergistic) interactions with security, both for how each one is addressed and over what time period.

The Milestones documents describe three phases of the process to develop this infrastructure:

1. Consideration before a decision to launch a nuclear power program is taken. This ends with Milestone 1: Ready to make a knowledgeable commitment to a nuclear program.
2. Preparatory work for the construction of a nuclear power plant after a policy decision has been taken. This ends with Milestone 2: Ready to invite bids for the first nuclear power plant.
3. Activities to implement a first nuclear power plant. This ends with Milestone 3: Ready to commission and operate the first nuclear power plant.

Phase 1 occurs before the facility lifecycle because it falls before the national decision to adopt nuclear power. During this phase, critical actions occur with respect to starting the project to build the first NPP, such as definition of the legal, regulatory, and environmental criteria associated with NPP/NF construction, operation, and dismantlement. The Milestones documents [1,2] recommend that the State form a Nuclear Energy Program Implementing Organization (NEPIO) to examine the issues and conditions necessary for successful implementation of nuclear power in the country. Initially the NEPIO would conduct pre-project activities to examine study the high-level requirements (the "what's") and determine the feasibility of adopting nuclear power. Considerations would be the capacity/capability of the NPP/NF, the potential sites for the NPP/NF, the infrastructure needs beyond existing, anticipated construction costs, and so on.

Phase 2 occurs before a bid is requested for the first nuclear power plant, so Phase 2 activities represent part of the pre-project activities before the NPP/NF project starts.

Note that the 18 non-security infrastructure issues in the Milestones documents can also be profitably reviewed by the security-oriented reader because many of these issues either have strong interactions with security, as in 3S, or their coverage in the documents provides insight about security. As examples:

- Funding and financing: By milestone 2, plans need to be in place to assure fully funded security and safeguards programs;
- Human resource development: By milestone 2, the majority of the technical and regulatory expertise to develop and implement physical security regulations, codes, and standards should be in place;
- Site and supporting facilities: Risks from man-made events (such as malevolent threats) are important elements of site study and characterization, planned and implemented over all three phases; and
- Nuclear safety: Many of the same issues of safety importance in constructing the first NPP are also important to security. As an example, the need for management competence to deal coherently with regard to safety is matched by a need for competence about security.

Thus, for all the reasons discussed here, the reader is strongly advised to review these two documents (references [1,2]).

More discussion concerning the Milestones documents is provided in the sections covering Fundamental Principle A: Responsibility of the State through Fundamental Principle D: Competent Authority.

The IAEA also released technical document that covers the milestones in more detail in reference [5]. In this document, Milestone 2 is preceded by site selection, environmental assessment, and site licensing. After Milestone 2 come steps such as bid evaluation, supplier selection, etc., leading to a construction license.

The International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) documents in reference [4] an assessment methodology for evaluating the use of an innovative nuclear energy system under a physical protection regime in a country that is planning to install a nuclear power program. This approach, though, is general enough to be useful for evaluating the quality of the physical protection regime for more conventional NPP designs. The approach considers such topics as security-related design features, security culture, contingency plans, and recovery of material and facilities. For each topical area, the assessment methodology provides a physical protection user requirement, such as “the innovative nuclear energy system component layout and design should be developed to minimize susceptibility and opportunities for malicious action,” then lists some criteria for determining how well that requirement is met (such as “Is there evidence that consideration has been given to physical protection in the design of the system’s components?”), and then discusses what factors should be considered in determining whether a particular criterion has been met (one such factor, out of several supporting whether physical protection has been considered, is whether or not the technology holder’s

design “reflects compartmentalized access to target locations to facilitate protection against the insider”).

It should be remarked that the Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group of the Generation IV International Forum [6] also documents an evaluation methodology for assessing the physical protection of the so-called Generation IV Nuclear Energy systems. This approach is more general than the INPRO approach but contains some useful ideas.

2.2 Assumptions

The following assumptions are provided to build a basis of understanding for this handbook; they are located just after the discussion of the milestones documents because they relate to phases in the development of a national infrastructure for nuclear power.

Assumption 1: The State has established, or is establishing, an effective nuclear regulatory framework and a competent authority to oversee and regulate nuclear power plants and facilities within the State. If a potential nuclear State does not have these in place, then it should take action to establish them prior to construction of a NPP or NF.

Assumption 2: The State has a stable and well-defined set of nuclear security laws and regulations, as well as effective competent authorities to license and perform oversight of the NPPs/NFs. This Handbook is specific to design principles and practices and does not cover the establishment of a legislative and regulatory framework.

Assumption 3: A Threat Assessment (TA) and/or set of PPS requirements are available and the competent authority has defined high radiological consequences and unacceptable radiological consequences. The official Design Basis Threat (DBT), if one exists, should also be available. These documents assume that there is a cost (risk) benefit to identifying SeBD concepts for threats beyond the current DBT.

Assumption 4: The PPT is familiar with project management and systems engineering processes. The specific details of these processes are not covered in this document.

While the Milestones documents call for measures that match these assumptions, SeBD assumes that some of the activities are completed earlier than stated in the Milestones documents. For example, SeBD assumes Assumption 3 is met before or at Milestone 2, while the Milestones documents assume Assumption 2 is met before or at Milestone 3, when the first plant is ready to be commissioned. Note that if the DBT is only in place when the plant is ready to be commissioned, then the security system design for the plant would have to be postponed past the early phase of the lifecycle where the real value of SeBD can be achieved.

3 Strategy for Achieving Security-by-Design

The basic strategy for achieving SeBD includes four main elements, each of which is described in more detail in this section of the Handbook:

1. Integrated Design Team: Incorporation of a PPT within the context of the overall design team, where the lead designer has responsibility for implementing Safety, Security, Safeguards, Operations, and Sustainability/Reliability, and is supported in carrying out that responsibility by the Project Leads in each of these areas;
2. Risk Informed Design: Use of a risk-informed design decision-making process that addresses threat, vulnerability, and consequence;
3. 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, from the earliest conceptual phases to facility dismantlement; and
4. 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 so that, in particular, early introduction of these principles into the design process will yield more efficient and effective results.

In general, SeBD is best achieved when the physical protection requirements are designed to be intrinsic to the concept, design, realization, and operation of a NPP or NF. Based on similar experience with safety by design (reference [7]) and safeguards by design (reference [8]), early application of these four elements to incorporate such intrinsic features in the facility design will be of maximum benefit to the overall security of the facility.

3.1 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 use of such a combined effort has been found to both reduce design time and to improve the quality of the integrated system in performing each of the functions. Additionally, such teams are ideal for incorporating systems engineering best practices and performing requirements analysis to best trade off the different functional requirements.

The integrated design team (shown schematically in Figure 3) 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). Note that we have assumed that the Lead Designer is responsible for integrating all of these functions; this is more likely to result in the designer seriously involving the Security Design Team at an early phase and continuing this involvement throughout the design and construction process. A similar responsibility, for the plant manager for example, can be assigned during operations and dismantlement and decommissioning.

Depending upon whether or not the facility is a fuel-cycle facility, there may be a need to have a process design team as part of, or separate from, the operations design team.

While this report focuses on SeBD, “by Design” processes have been developed for most of the other topical areas. For example, see reference [9] for a process for integrating safety into the design process, as well as some lessons-learned from using that integration process (reference [10]). Many of the lessons-learned from safety and international safeguards-by-design are useful for security also.

An important topic is how to employ an Integrated Design Team to coordinate the five functions shown in Figure 3 during facility design and operations. The functions of each design team are shown below the appropriate design team name.

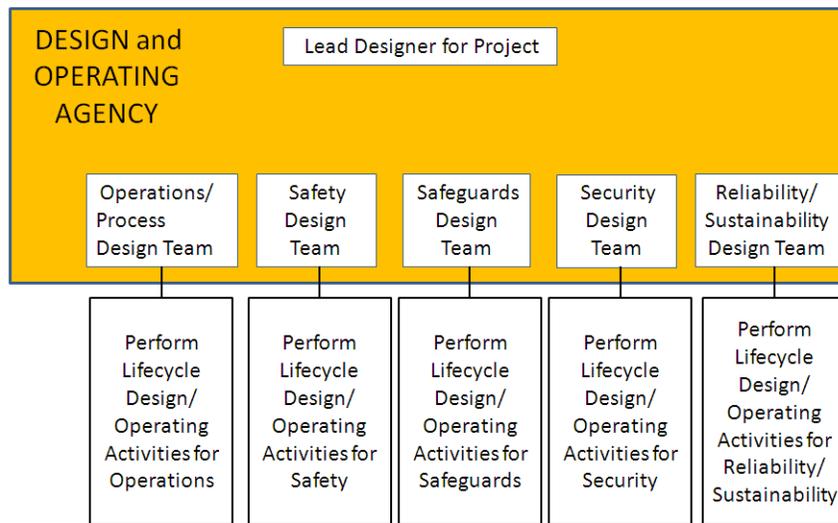


Figure 3. Integrated Design Team

In Table 1, each of the design-team functions listed in Figure 3 is cross-referenced with the other four. The X’s refer to particular interactions between these functions, while the “3S” and “SBD” refer to specific clusters of functions that have been addressed in the references to this handbook.

Table 1. Interactions between the Five Integrated Design Team Functional Areas

	Safety	Safeguards	Security	Reliability/ Sustainability
Operations/ Process	X	X	X	X
Safety		3S	3S	X
Safeguards			3S, SBD	X
Security				X

The interactions indicated in this table will now be discussed individually.

The Operations/Process function (top row of Table 1) has a great impact on the other four functions because it defines what operational states (of interest for all the other four) exist at the facility. Each of the operational states may require different people, procedures, and equipment; operational or production processes; types and throughput of material (for safeguards and security purposes); types and numbers of personnel, vehicles, and equipment that need to enter the facility at one time (for security purposes); and different requirements for equipment reliability to meet the operational mission.

As can be seen in the second row of Table 1, the Integrated Design Team must balance Safety, Safeguards, and Security (3S) functions as well as reconcile all safety, safeguards, and security disciplines to ensure sufficiency in each. There is substantial literature on this topic, and references are provided later in section 4.20 Other SeBD Principles – Synergy between Safety, Safeguards, and Security. There is also a paper, reference [11], which specifically discusses the integration of Safeguards and Security with Safety in the design phase.

The SBD in the table refers to Safeguards-by-Design, as defined by Idaho National Laboratory (INL). INL's definition of SBD not only includes safeguards but also physical security and cyber security. This SeBD handbook does not address cyber security.

Reliability/Sustainability (fourth column of Table 1), while being an important topic in its own right, affects safety (as certain systems may fail during or have failed before a safety incident), safeguards (removal of material or tampering may occur when systems fail), and security (security systems need to be operating 24/7). Reliability Centered Maintenance (RCM), along with the collection of reliability and availability data, has been an important activity within the nuclear industry for over 20 years.

A straightforward and simple integration plan incorporating security and shared among the design teams is valuable as part of the overall Project Plan. Such a plan identifies required activities with their timeline and provides detail and analyses at each phase of the design cycle. From this perspective, the handbook descriptions of the design process and associated activities can form a basis for developing such a plan.

3.2 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. In many cases, the competent authority requires some sort of documented risk assessment. At the same time, modern systems engineering approaches for designing and constructing facilities explicitly include risk management as one of their important processes. Effective security designs are developed around good estimates of the threats, whether from external (or outsider) sources or internal (or insider) threats. The current threat is difficult to predict in a definite fashion, much less predicting the threat over the lifecycle of a facility that may stretch 60-80 years into the future. For this reason, designs should be flexible to allow for additional security capabilities to be added in the future as suggested, perhaps, by future risk

assessments. Note that a later section, “Possible Areas Where the DBT/TA Capability May Increase in the Future,” provides some general suggestions about how this might evolve in the future.

This section first defines the term “risk informed,” then discusses how risk is used as a key factor in the decision-making process for designing and evaluating physical protection systems, and finally discusses how security risk is determined.

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 risk-informed design decision-making process, described below, addresses threat, vulnerability, and consequence. The process has two major two 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 risk process and the design approach are discussed below. The the high-level steps of the design and evaluation process (DEPO) are shown in Figure 9. This process is adapted from the version of DEPO in reference [12] by explicitly adding the step, “Establish Facility Design Options.”

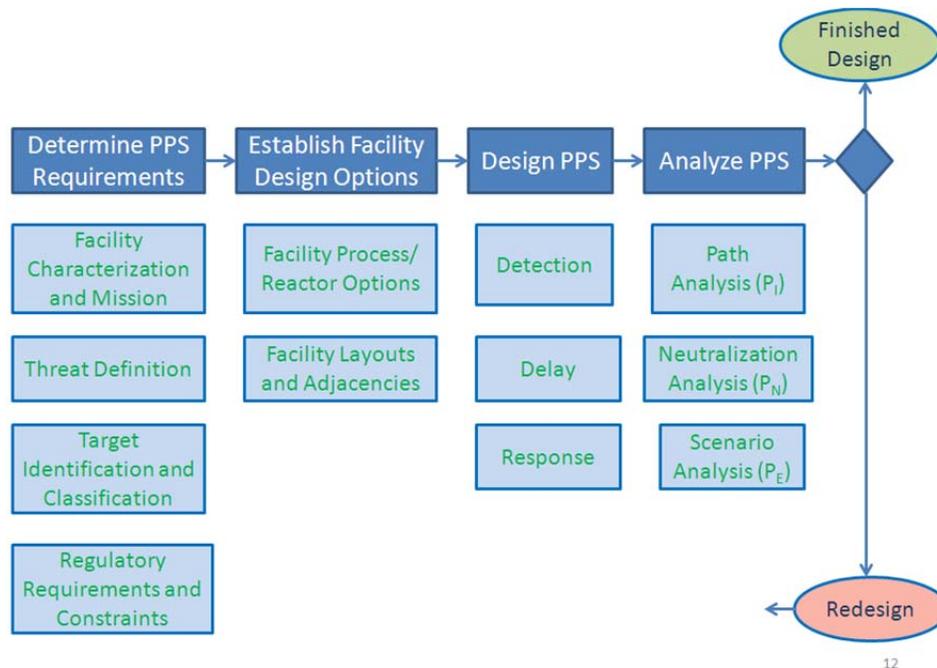


Figure 4. Design and Evaluation Process

The analysis of the PPS design needs to assess the effectiveness of the PPS itself, 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.

The Probability of System Effectiveness can be expressed quantitatively when sufficient data exist, or it can be expressed qualitatively. One quantitative model is a product model relating three parameters:

$$P_E = P_I * P_N$$

where

P_I = Probability of Interruption, which is determined as part of what is called Path Analysis; and

P_N = Probability of Neutralization, which is typically determined as part of Neutralization Analysis, performed on paths developed by Path Analysis.

The Scenario analysis step typically attempts to determine P_E directly, either qualitatively or quantitatively. The probabilities P_I and P_N are defined slightly later in this subsection.

The design and evaluation of the PPS must be done from a system standpoint, providing detection, delay, and response, properly weighted to their contributions to the PPS. At a high level (i.e., the decision-maker or site-management level), the effectiveness of the PPS (and thus the design requirements necessary to achieve that effectiveness) must be balanced against available resources. The effectiveness of the PPS is incorporated within a risk-informed approach and is used to balance resource requirements versus benefit in providing protection.

Requirements are an important aspect of good systems engineering processes. Effective and efficient PPS designs occur when design requirements have been established and are known as early as possible in the lifecycle. To achieve good early requirements more effectively, the State should seek the guidance of physical protection experts in their pre-project deliberations affecting site locations and potential distribution of NPP and NF within their country, even before the NPP/NF project commences.

The PPS objectives and requirements for the facility can be derived by the designer from applicable regulations by the competent authority. This would include an understanding of:

- What is to be protected (the What?)
- The threat against the facility (the Who?)
- Protection objectives for the facility (How Well), which depends upon the consequences of sabotage attack, the type of nuclear material stolen, etc.

The security risk for a facility associated with malevolent activities is given by:

$$R = P_A * (1 - P_E) * C,$$

where:

R = Risk to society of an adversary gaining access to, or stealing, nuclear material.

P_A = Probability of adversary attack. It is very difficult to determine what this value should be. Clearly, simple use of past history to estimate this value may not be appropriate, given the current understanding of today's threat environment.

P_E = Probability of system effectiveness, representing the probability that the PPS prevents the consequence given an attack.

C = Consequence associated with the loss of the targets the PPS is designed to protect. For a nuclear power plant, the consequence is typically associated with a radiological release.

In the product model for P_E , $P_E = P_I * P_N$,

P_I = Probability of interruption. This is the probability that the defined adversary will be interrupted by the response force in time to stop the adversary from accomplishing his objectives.

P_N = Probability of neutralization. For a given adversary and response force, given an interruption has occurred, this is the probability that the response force will defeat the adversary in an engagement (i.e., prevent the adversary from accomplishing his objective).

Consequence measures can be based on other aspects of an attack, such as whether or not core damage occurs. The appropriate consequence measure to be used in the PPS risk calculation is established by the competent authority.

Typically, during the design of PPS, the assumption is made that an attack occurs. Thus, the risk equation becomes:

$$CR = (1 - P_E) * C$$

where

CR = Conditional risk (i.e., the risk given an attack).

The focus of the PPS design process is on minimizing CR through minimizing the consequence (C) and maximizing P_E .

Appendix B discusses a more detailed approach for addressing security risk that can be extended to cover the risks associated with all components of 3S.

3.3 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. This section starts by describing a baseline structure for how the facility goes through various phases making up the facility lifecycle, from pre-conceptual planning to design, construction, operations, and dismantlement. It also describes both security and non-security activities that occur during each lifecycle phase. Then, this section provides examples showing how the activities by the State, Design and Operating Agency, and the PPT are organized and interact during each lifecycle phase; note that this discussion provides some explanation of how the Security by Design Generic Design Process described in Appendix A is organized. Along the way, the section includes an overview of how security design or evaluation activities compare from phase to phase of the lifecycle; this comparison is summarized in Table 2 on page 36.

The lifecycle of NPPs and NFs are complex and involve an ongoing interaction between the State, the Design and Operating Agencies, and the PPT. Clearly, projects are highly detailed, as are the regulatory structures and specific technical elements underlying the PPS design, construction, and operation. Hence, the descriptions of the phases presented below are abstracted to focus on key process activities and interactions.

For the purposes of this document, 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. In this document, this phase includes 1) State activities before the NPP/NF project is initiated to develop the national infrastructure for nuclear power, development of regulations for constructing, operating, and dismantling the NF (for security, this would include grading requirements), and site selection and design scope review; and 2) Project-related activities by the Design and Operating Agency to support a decision on whether or not to approve the project.
- **Design Concept Phase** starts by defining the lifecycle requirements for the facility and the mission need statement, which includes the project team's assessment of the gap between desired and existing capability (e.g., a need for nuclear power), the scope of the need, associated potential hazards arising from nuclear material, and a rough order-of-magnitude assessment of NPP/NF project cost and schedule. During conceptual design, various design options are considered to determine how well these meet design requirements and demonstrate efficiency. By the end of this phase, a conceptual design would be selected.
- **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. Commonly, a project execution plan

(PEP) is developed describing the design objectives, schedule, and cost, as well as project roles and responsibilities.

- **Contracting Phase** assumes that an Architecture and Engineering (A&E) firm was selected after project approval to develop the design 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, the site goes through formal acceptance procedures, and (if this is completed successfully), management transfers from the project-management team to the site-management team.
- **Fitness-to Operate-Phase** is the phase in which the competent authority conducts a “Fitness to Operate” evaluation. If this is completed successfully, then the competent authority will permit or license the NPP/NF to enter full, unrestricted operations.
- **Plant Operations Phase**, where the facility operates normally until a decision is reached to cease operations.
- **Decommission and Dismantlement Phase**, where decisions may be reached to remove any remaining nuclear material inventory, part or all of the NPP/NF is environmentally restored, and decisions are reached as to how to dismantle the NPP/NF.

Note that the project phases, from scope and planning to construction, can also be viewed from a project management perspective; for this viewpoint, see the Project Manager’s Body of Knowledge (PMBok), reference [13].

Figure 5, below, structures and depicts the lifecycle for facility design and operations, as the facility proceeds from pre-conceptual planning to design, construction, operations, and dismantlement. The lifecycle description provided here is very much simplified from what is used in practice. This simplified version is provided for reference when using this handbook for identifying what physical security activities need to be performed and where the SeBD principles and practices can be applied during the lifecycle.

The actual project lifecycle for a facility occurs within the context of a developing or an existing national infrastructure for nuclear power within the State and is beyond the scope of this handbook. The IAEA Milestones Documents [1,2] Context for Security By Design subsection and The INPRO Assessment Methodology [4], Section 2.0, briefly describe the three milestones indicated in Figure 5 and Figure 6 as IAEA M/S 1, 2 and 3.

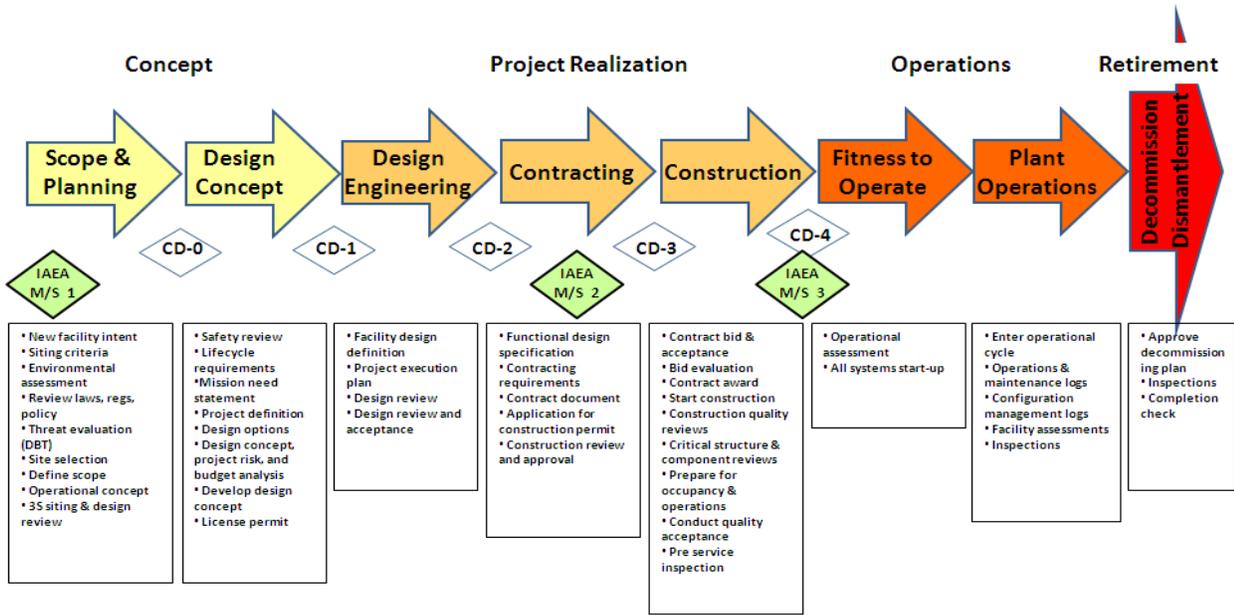


Figure 5. Facility Design/Operations Lifecycle

Figure 6 below shows the same lifecycle diagram as in Figure 5, but annotated with the activities specific to the PPT shown in red font.

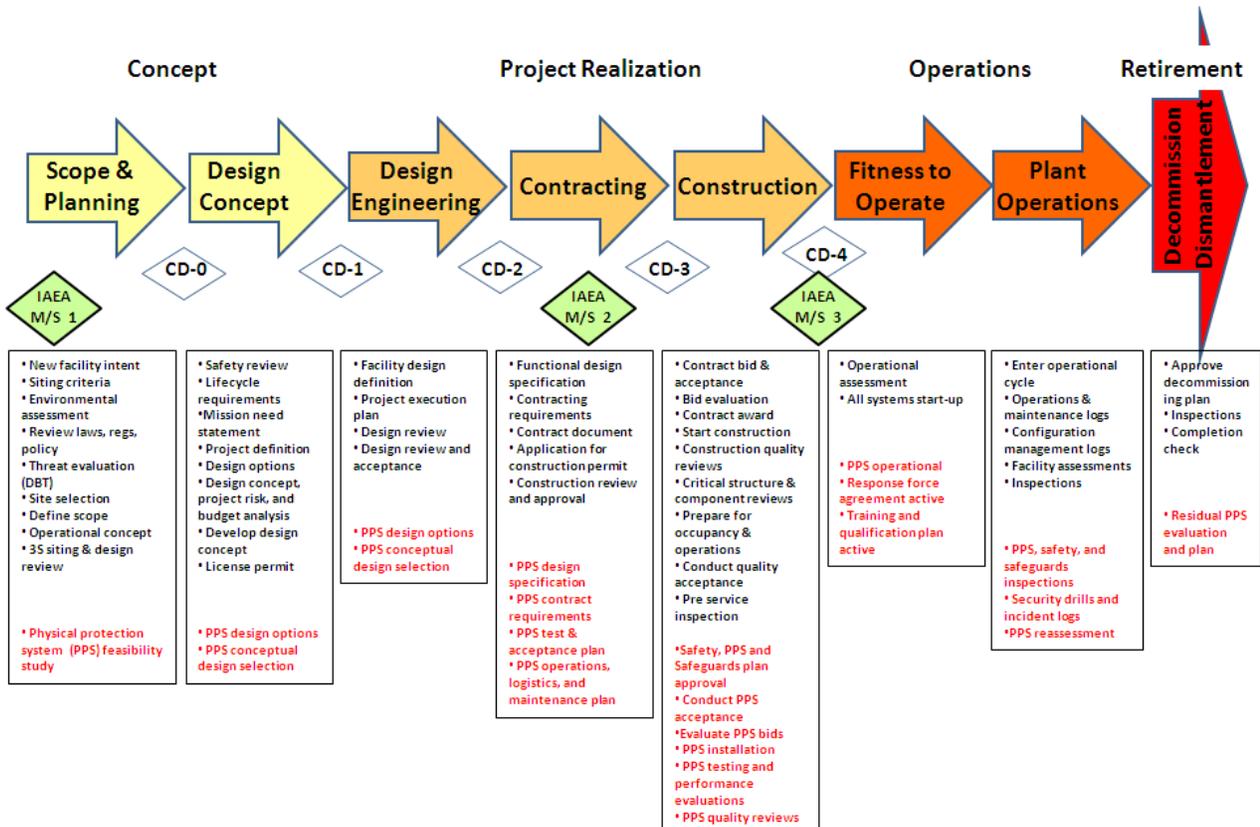


Figure 6. Facility Design/Operations Lifecycle with Focus on the Security Dimension

For SeBD, the threat and protection objectives as well as the stage regulations, must be clearly defined before the conceptual design phase can commence; this is discussed in more detail in Section 3. First, the design is developed in terms of facility requirements definition started during scoping and planning, then conceptual design, and finally engineering design. The engineering design can be matched more easily to the graded requirements defined by the State, covering both theft and sabotage. Critical areas and systems of the PPS may need to be protected at a level exceeding requirements that are based solely on material categorization or whether a sabotage release exceeds Unacceptable Radiological Consequence levels or High Radiological Consequences.

An important aspect of the project-related scoping and planning, and design concept phases is tradeoff analysis between the Integrated Design Team's five functional areas (Operations/Process, Safety, Safeguards, Security, Reliability/Sustainability in Figure 3). Early trade-off analyses can identify cost savings or synergies between the different functions, as well as regulatory requirements that drive up costs or produce conflicts. These may merit review/modification by the competent authority.

While this lifecycle is for the facility as a whole, it should be recognized that subsystems of the NPP/NF may be operating in different lifecycle phases at a given point in the facility lifecycle and, thus, their actual implementation may occur at different times; for example:

- In a nuclear power plant, the Nuclear Island (Nuclear Steam Supply System, or NSSS, and Balance of Nuclear Island, or BNI) and the Turbine Generator are typically provided by a vendor and are therefore in a further stage of design than the rest of the plant (Balance of Plant).[14]
- Subsystems, such as the Electronic Security System in the PPS, have different lifecycles (e.g., five years), so the design should accommodate upgrading and replacing such systems. Similar concerns may exist for certain structures at the facility.

The lifecycle phases can be categorized into lifecycle stages, each of which includes one or more lifecycle phases. This categorization is employed in Section 4, Principles and Practices, to describe principles and practices that apply over multiple lifecycle phases. The lifecycle stages are defined as follows:

- **Concept Stage** encompasses all activities beginning with a facility mission need statement. It includes State requirements definition, threat assessment, and physical protection objectives. The output is sufficient information to allow facility project initiation. Security "theme" (the answers to how security will be implemented (people, equipment, and procedures), including defining limitations, such as who provides armed response) emerges. Reliability, availability, and maintainability analyses may be performed at this stage.
- **Realization Stage** is the set of activities, including project management, system engineering, design, quality assurance, and procedural definition, that lead to construction, commission, and operational readiness. The security theme matures and becomes well-defined. Security operational procedures and concept of operations are written and validated.
- **Operations Stage** is the recurring set of actions for the functioning and sustainment of the physical protection system, resulting from the interplay of people, processes, and technology. The security theme is fully functional and can be assessed.

- **Retirement Stage** (also known as Decommissioning and Dismantlement) is the set of actions required to decommission a facility.

Table 2 shows how the lifecycle phases from Figure 5 and Figure 6 align with these four lifecycle stages. Note that this document includes “Siting” in the Scope and Planning lifecycle phase, so the siting line is conceptually redundant; it is present here to match Figure 6.

Table 2. Lifecycle Phases and Associated Project Activities

Lifecycle Stage	Lifecycle Phases
Concept	Siting
	Scope and planning
	Design Concept
Realization	Design (Engineering and ConOps)
	Contracting
	Construction
Operations	Fitness to operate (Validation)
	Plant Operations
Retirement	Decommission
	Dismantlement

One example of a lifecycle process is shown in Figure 7; this process has been adopted from the Japan Atomic Energy Agency (JAEA) process used for a NPP until recently. Red lettering denotes the specific activities for physical protection (for example, “PP Plan”). Figure 7 lists three entities side-by-side. They are the operator, which may be the Design and/or Operating Agency; the METI/NISA³ (Ministry of Economy, Trade, and Industry/Nuclear and Industrial Safety Agency); and the Japan Nuclear Safety Commission.

³ Historically, the METI/NISA mission was to ensure the safety of industrial activities and individual facilities. Later the METI/NISA broadened their mission to include physical protection so in this (dated) figure, they represented the State’s competent authority and served as the principal licensing and inspection agency.

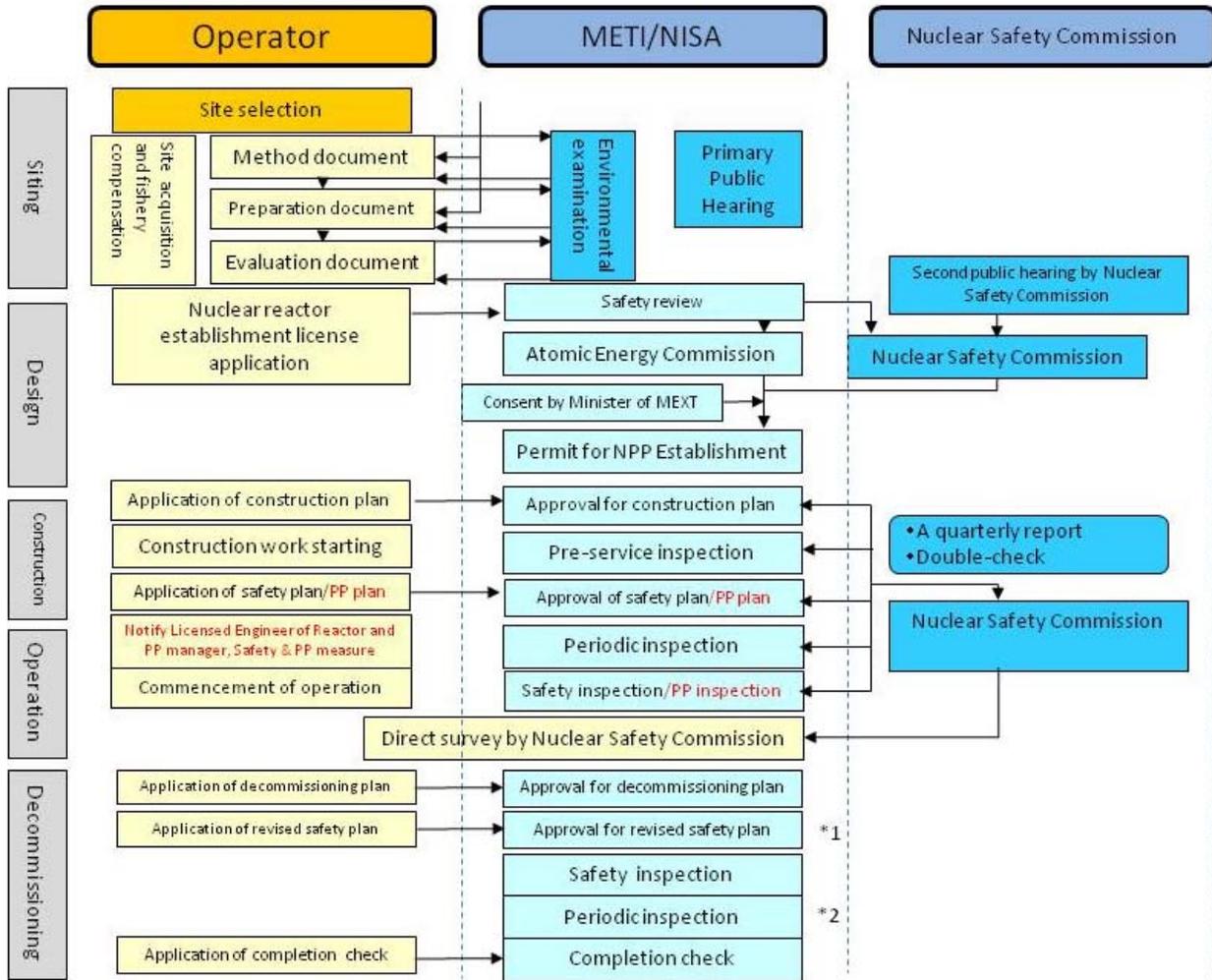


Figure 7. Japanese Implementing Procedure for Nuclear Power Plants

In developing a notional lifecycle for this document (Figure 8), critical decisions (CD) serve to delineate transition from one phase or project element to the next. For example, the diamond with "CD-0" marks the transition from the Scope and Planning project element to the Design Concept project element. The IAEA phase milestones are comparable to phase CDs, and Figure 8 includes them for comparison to the notional lifecycle phases. The circled items in Figure 8 indicate where a Design and Evaluation Process Outline (or DEPO) assessment is performed for the security system (this DEPO assessment was described in more detail in Section 3.2, Risk-Informed Design). The vertical bars on the schematic compare the IAEA and notional lifecycle phases.

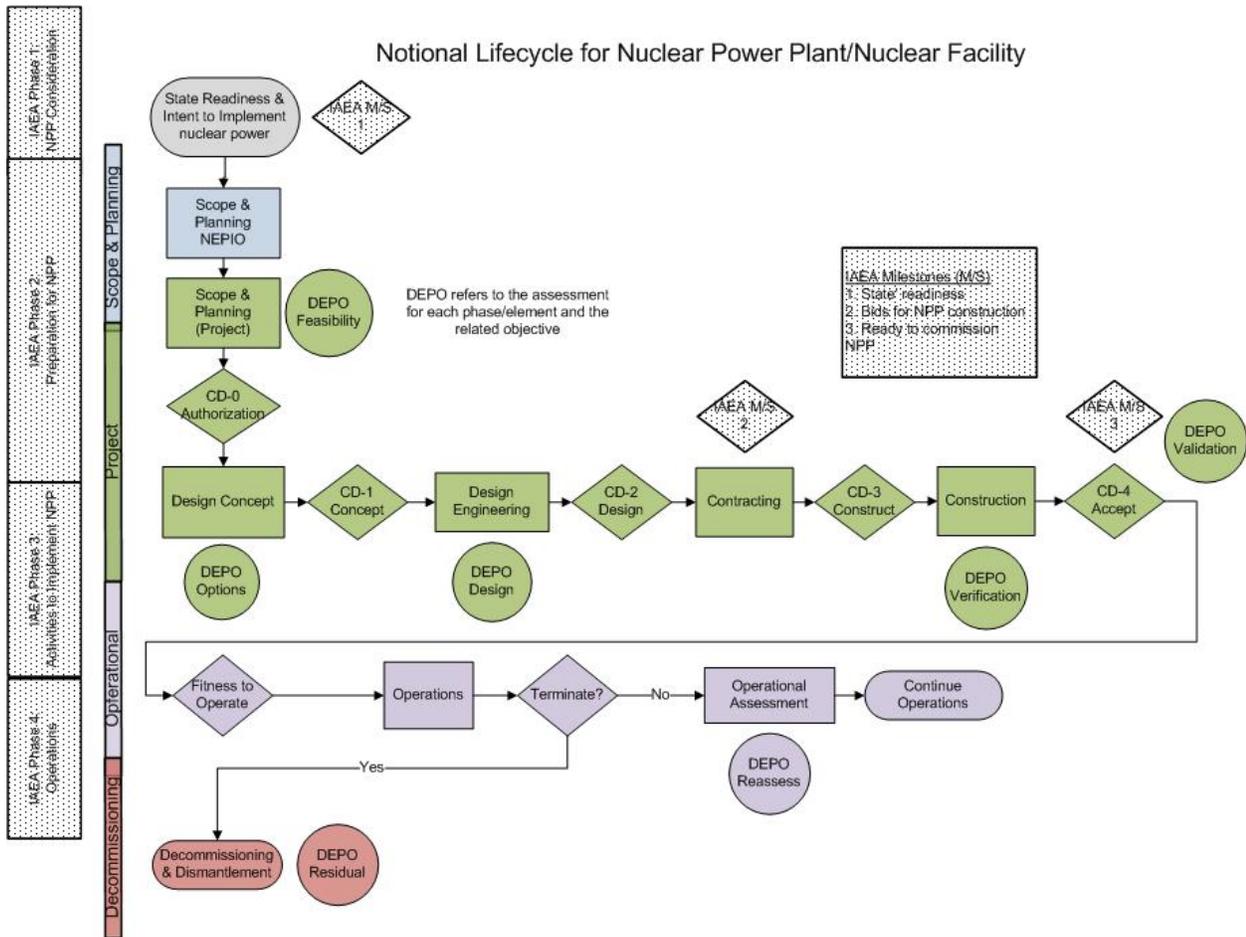


Figure 8. Diagram of Notional Lifecycle⁴

Table 3 summarizes the lifecycle assessments from Figure 8 and their objectives. Typically, the related DEPO assessments are tailored in rigor and key objective, based on the phase or project element. For example, during the Scope and Planning phase prior to CD-0, the PPT conducts a DEPO assessment as part of security feasibility study, focusing on broad PPS objectives and conceptual design requirements. While the State may provide a DBT, the possibility exists that one has not been published. In this instance, the PPT might work with the competent authority to develop an approved threat assessment for the PPT to plan against. Using either the threat assessment or the DBT, the PPT study examines the location and adequacy of potential sites and response forces. The outcome is a high-level feasibility assessment describing the acceptability of potential sites, response force plans, and a qualitative estimate of PPS effectiveness based on these considerations.

⁴ NEPIO is the State’s nuclear energy program implementing office. It is placed in the diagram to illustrate the State’s role and transition point in the Scope and Planning for a new NNP/NF.

Table 3. Assessments in Lifecycle

Phase/Element	DEPO Assessment Objective	Occurs before
Scope and Planning	<u>Feasibility</u> : Assures principal design requirements are consistent with mission need <u>Protection Strategy</u> : Investigate Protection Strategy	CD-0 Project Authorization
Design Concept	<u>Options</u> : Evaluate and choose among competing facility and PPS design approaches	CD-1 Design Selection
Design Engineering	<u>Design</u> : Final PPS design consistent with 3S priorities	CD-2 Design Approval
Contracting	None	NA
Construction	<u>Verification</u> : Quality assurance that PPS design achieves security objectives	CD-4 Acceptance
Fitness to Operate (Acceptance)	<u>Validation</u> : System assurance of PPS, operators, and response force for entry into operations	Operations Approved
Operations	<u>Reassessment</u> : Verification PPS performs as designed and remains consistent with threat	Operational Inspections & Assessments
Decommission & Dismantle	<u>Residual</u> : Determine residual PPS requirements post operations	

Figure 9 provides a logical depiction of a feasibility assessment. In this example, the PPT might study what delay requirements for the facility, specified as X minutes of delay, are actually large enough to allow offsite Response Forces to arrive in time to interrupt the adversary. The security requirements would then be considered feasible if the PPT believes that X minutes of delay are achievable in the design, and an adequately sized response force can arrive within that time.

As another example, during the conceptual design project element, the PPT develops options and again uses a DEPO assessment to evaluate the merits of each design option qualitatively. The PPT should analyze the PPS options with sufficient rigor to characterize and allow selection of a preferred option. Any assessment will likely be very high level but insufficient for the final design.

As a third example, following option selection at CD-1, the PPT completes the more detailed design engineering and completes a more comprehensive analysis of the design. In this case, the PPT will either complete the final design or redesign to correct deficiencies. Once this is resolved, the PPT releases the final design to the project team responsible for design, construction, and acceptance of the NPP/NF. From this point and onward, PPS changes become increasingly costly and difficult to implement. A comprehensive security analysis of the PPS is essential, and the project team should reconcile potential 3S conflicts.

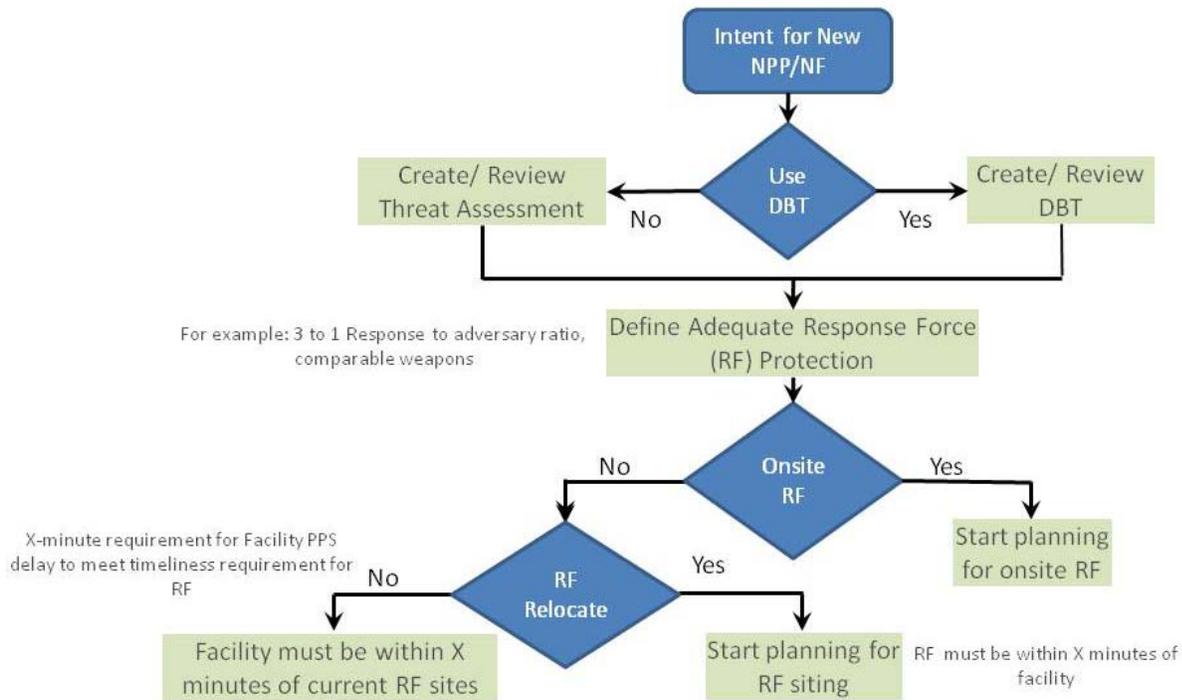


Figure 9. Feasibility Study Logic Flow

Figure 10 depicts the essential notional lifecycle actions to achieve SeBD by the three key entities: State, Design and Operating Agency, and Physical Protection Team. Placing them in side-by-side columns allows comparison of relative time, precedence, and dependencies. The authors did not attempt to define decision makers or to define timelines. Definition of these would occur when needed and are highly conditional on factors well outside the scope of this document. Note that the project team is portrayed in this document as being an entity within the Design and Operating Agency.

Figure 10 shows an example of how the Design and Operations, and PPT activities under each project phase can be described, ordered, and related to one another in more detail. Note that Figure 6 shows only activities specific to the PPT; other design teams would have ongoing parallel activities, and there would be interactions between the teams. Appendix A includes figures similar to Figure 10 that show the activities for the State, the Design and Operating Agency, and the PPT across all of the lifecycle phases.

Project Phase: Design Engineering			
Project Element	State	Design and Operating Agency	Physical Protection Team
Project Execution Plan			PPS Design
			ConOp
			Training and Qualification Plan
			Response Force Agreement
Manage Design	Design Review and Acceptance	Facility Design Definition	
		Project Execution Plan	
		Design review	
			DEPO: Design (final)
CD-2: Design Approval			

Figure 10. Design and Operations Activities for the Design Engineering Phase

Some general comments follow on SeBD and the design process:

- The NPP/NF site location may impose additional security constraints and limitations on PPS effectiveness. Physical protection experts should provide their input to site identification as part of the Scope and Planning phase to take advantage of site features to reduce costs and achieve a more effective PPS.
- Initially, the Scope and Planning phase occurs outside of the project, but with the State's declaration to develop a NPP/NF, the Scope and Planning phase ends and the NPP/NF enters the project phase. At this time, Scope and Planning becomes a project element.
- Concurrent with Project Definition, the PPT examines PPS options and conducts a preliminary risk analysis of each option. This PPT activity allows the PPT to evaluate potential designs with respect to meeting physical protection objectives. (Typically, these studies will form part of comprehensive 3S studies covering the options.)
- When the project team selects the preferred NPP/NF design option, the PPT should validate the chosen PPS option Design and Evaluation Process Outline (DEPO) analysis and validate that it is current. Once validation is complete, along with other reviews such as safety and safeguards, the project team submits their design to the competent authority and Design and Operating Agency for "conceptual design" acceptance and continuation into the Design Engineering phase.
- The PPT, working with the project team, should create the Concept of Operations (ConOps), response force plans, and finally the training and qualification plan. These are source documents

for later site acceptance and continuous operations. All such plans must be under configuration management.

- The physical protection objectives, the design basis threat, and State regulations are fundamental to a PPS design. Defining the objectives and threat occur early during the Scope and Planning phase, and are pre-project activities.
- Prioritization between potentially competing 3S requirements must occur in a systematic, consistent, and auditable manner, allowing assurance to the competent authority that the NPP/NF conforms to the State's laws, regulations, and environmental criteria.
- The adoption of standards and commonly accepted practices are strongly advised to reduce project risk. Such standards and practices include quality assurance, configuration management, and project management. During transition to operations, the PPT working with the project lead should assure the quality and configuration management systems transition seamlessly to the operational phase. During design, the PPT should consider definition of recurring security exercises and assessments for use throughout the NPP/NF operational life. Such action should also include a definition of essential performance logs allowing later operational assessment and trend analysis. This is becoming increasingly important data for use in reliability, availability, and maintainability assessments.

4 SeBD Principles and Practices

The principles and their associated practices for SeBD are described in this section. If adopted, these principles and practices are expected to provide high confidence in both the effectiveness and sustainable operation of the PPS. This 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 [3], so that the section describes useful practices that support each of the 12 Fundamental Principles. The Principles identified in this document are the irreducible set of requirements describing the “what.” Practices, the “how,” provide information such as processes, methods, or technologies to meet the set of principles. These could include commonly used procedures captured in a design guide or a standard used to gain uniformity.

Discussions for each principle have been kept fairly brief and were limited to one or two pages. Where additional material has been collected relevant to a principle, it has been incorporated within an appendix to the handbook.

Each of the 12 Fundamental Principles is covered in this section. 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.

The section continues by discussing a number of what are called “other” SeBD principles (these are listed as “other” as they are not included as one of the 12 Fundamental Principles). These correspond to:

- Employing good approaches to design (such as incorporating what is called “intrinsic security”);
- Following proven engineering, project management, operational planning, and systems engineering principles;
- Taking project perspectives that consider both the facility lifecycle and the different facility conditions called for in the concept of operations,
- Considering integration and synergy between safety, domestic safeguards, and security (3S);
- Designing-in PPS sustainability;
- Balancing prescriptive and performance-based requirements through cooperation between the design team and the competent authority;
- Validating effective communication and/or operational agreements with other agencies, such as police and the military; and
- Making use of project and operations experience to incorporate lessons-learned;

Note that Section 5, provides some details on how the SeBD framework, including the principles and practices, has been and can be applied.

4.1 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.

The **physical protection regime** is defined as “A State’s regime including: the legislative and regulatory framework governing the physical protection of nuclear material and nuclear facilities; the institutions and organizations within the State responsible for ensuring implementation of the legislative and regulatory framework; facility and transport physical protection systems.”

More details on this element of the physical protection regime, as well as associated practices, can be found in paragraphs 3.1 and 3.2 of INFCIRC/225/Revision 5 [3].

The earlier discussion in section 2.1, Context for SeBD within the Milestones Documents and the INPRO Assessment Methodology, discusses the establishment and implementation of a physical protection regime as part of the process for developing the infrastructure necessary to support a nuclear power program and describes three phases of the process to develop this infrastructure, as defined in the Milestones Documents [1,2]:

1. Consideration before a decision to launch a nuclear power program is taken. This ends with a milestone, Milestone 1: Ready to make a knowledgeable commitment to a nuclear program.
2. Preparatory work for the construction of a nuclear power plant after a policy decision has been taken. This ends with a milestone, Milestone 2: Ready to invite bids for the first nuclear power plant.
3. Activities to implement a first nuclear power plant. This ends with a milestone, Milestone 3: Ready to commission and operate the first nuclear power plant.

Based on these considerations, the pre-project team should develop a Scope and Planning document describing the high-level operational concept and the related factors allowing grading by the NPP/NF project team.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
Management Principles and Associated Practices									
FUNDAMENTAL PRINCIPLE A: <i>Responsibility of the State</i> : 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

4.2 Fundamental Principle B—*Responsibilities during International Transport*

The responsibility of a State for ensuring that nuclear material is adequately protected extends to the international transport thereof, until that responsibility is properly transferred to another State, as appropriate.

The transport is defined as “International or domestic carriage of nuclear material by any means of transportation, beginning with the departure from a nuclear facility of the shipper and ending with the arrival at a nuclear facility of the receiver.”

More details on this element of the physical protection regime can be found in paragraphs 3.3 to 3.8 of INFCIRC/225/Revision 5 [3]. Note that this principle will not be discussed further here, because transportation falls outside of the scope of this document.

4.3 Fundamental Principle C—*Legislative and Regulatory Framework*

The State is responsible for establishing and maintaining a legislative and regulatory framework to govern physical protection. This framework should provide for the establishment of applicable physical protection requirements and include a system of evaluation and licensing or other procedures to grant authorization. This framework should include a system of inspection of nuclear facilities and transport to verify compliance with applicable requirements and conditions of the license or other authorizing document, and to establish a means to enforce applicable requirements and conditions, including effective sanctions.

More details on this element of the physical protection regime can be found in paragraphs 3.9 to 3.17 of INFCIRC/225/Revision 5 [3].

The earlier discussion in section 2.1, Context for SeBD within the Milestones Documents and the INPRO Assessment Methodology, discusses the establishment and implementation of a physical protection regime, including the legislative and regulatory framework, as part of the process for developing the infrastructure necessary to support a nuclear power program, and describes three phases of the process to develop this infrastructure, as defined in the Milestones documents [1, 2]:

1. Consideration before a decision to launch a nuclear power program is taken. This ends with Milestone 1: Ready to make a knowledgeable commitment to a nuclear program.
2. Preparatory work for the construction of a nuclear power plant after a policy decision has been taken. This ends with Milestone 2: Ready to invite bids for the first nuclear power plant.
3. Activities to implement a first nuclear power plant. This ends with Milestone 3: Ready to commission and operate the first nuclear power plant.

Practice Associated with this Principle: Develop a balanced set of prescriptive and performance physical protection requirements, along with methodology for providing grading or compliance relief to achieve an efficient and effective Physical Protection System (PPS).

Note that this requires that physical protection requirements and a graded protection scheme be in place before the facility planning begins.

The CA and the license holders/design agency should mutually understand the requirements and how the CA will evaluate and inspect the NPP/NF, and what deliverables or documents need to be in place. The PPT should understand how the PPS design meets security requirements under the graded security approach. This mutual understanding is also beneficial when considering what design features can be incorporated to allow for future upgrades.

	Lifecycle Phases								
FUNDAMENTAL PRINCIPLE C: <i>Legislative and Regulatory Framework</i> Principle and Associated Practices	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
Principle: The State is responsible for establishing and maintaining a legislative and regulatory framework to govern physical protection. This framework should provide for the establishment of applicable physical protection requirements and include a system of evaluation and licensing or other procedures to grant authorization. This framework should include a system of inspection of nuclear facilities and transport to verify compliance with applicable requirements and conditions of the license or other authorizing document, and to establish a means to enforce applicable requirements and conditions, including effective sanctions.	Framework in place before Scope and Planning	X	X						
Practice Associated with this Principle: Develop a balanced set of prescriptive and performance physical protection requirements, along with a methodology for providing grading or compliance relief to achieve an efficient and effective Physical Protection System (PPS).	Requirements and grading in place before Scope and Planning	X	X						

4.4 Fundamental Principle D—Competent Authority (CA)

The State should establish or designate a competent authority, which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence, and financial and human resources to fulfill its assigned responsibilities. The State should take steps to ensure an effective independence between the functions of the State’s competent authority and those of any other body in charge of the promotion or utilization of nuclear energy.

More details on this element of the physical protection regime can be found in paragraphs 3.18 to 3.19 of INFCIRC/225/Revision 5 [3]. Note that this principle concerning the competent authority has no specific practices associated; the Milestones documents [1,2] discuss some desirable features for such an authority, such as the need for it to have a clearly-defined legal status and be independent from applicants/operators/shippers/carriers.

Practice Associated with this Principle: The PPT and the Design and Operating Agency should work closely with the CA to ensure that requirements are clearly defined and mutually understood, and that acceptance criteria are clearly defined.

In this regard, the PPT, and Design and Operating Agency must have a clear understanding of the deliverables and expectations of the CA during the design process.

FUNDAMENTAL PRINCIPLE D: <i>Competent Authority (CA)</i> Principle and Associated Practices	Assumptions	Lifecycle Phases							
		Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
Principle: The State should establish or designate a competent authority, which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence, and financial and human resources to fulfill its assigned responsibilities. The State should take steps to ensure an effective independence between the functions of the State’s competent authority and those of any other body in charge of the promotion or utilization of nuclear energy.	Competent Authority fully functional before Scope and Planning	X	X	X	X	X	X	X	X
Practice Associated with this Principle: The PPT and the Design and Operating Agency should work closely with the CA to ensure that requirements are clearly defined and mutually understood, and that acceptance criteria are clearly defined.		X	X	X	X	X	X		

4.5 Fundamental Principle E—Responsibility of the License Holders

The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licenses or of other authorizing documents (e.g., operators or shippers).

License holders are defined as either operators or shippers. More details on this element of the physical protection regime, as well as associated practices, can be found in paragraphs 3.23 to 3.30 of INFCIRC/225/Revision 5 [3].

The term “license holders” refers to the organization authorized by the State to build and operate NPPs or NFs. The license holders are obliged to follow the regulations and implement the various elements of physical protection at their facility. They have to interpret and convert all obligations stated in the regulation into requirements that then are incorporated in the design. For example, when the regulations say “put a double fence around the facility and guards should check all entering individuals to see if they are authorized,” the license holders implement that requirement accordingly. In many cases, license holders order an engineering company to do the design work, but the final decision is theirs. Put another way, the license holders realize physical protection measures as stated in the regulation by the government.

Not all requirements can be stated explicitly in the State’s regulations, specifically, the kinds of the requirements that reflect best-practice physical protection design concepts. For example, if all important buildings, from a security perspective, are placed in the limited area, surrounded by a fence that separates them from the offices, then physical protection of the plant will improve. Typically, though, this kind of requirement is too general to be incorporated within regulations, so it only can be realized by the License Holders voluntarily.

When the license holders have designed and operated a similar facility in the past, they can provide good advice from their experience to the regulator.

Note that this principle concerning the competent authority has no specific practices identified here. There are two points, though, to emphasize here:

- The prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licenses or of other authorizing documents; this means that the licensee is ultimately responsible for the effectiveness of the response force (as it supports the PPS effectiveness), as covered by the principles “Fundamental Principle K—Contingency Plans” and “Other SeBD Principle—Validate Effective Communication and/or Operational Agreements with Other Agencies.”
- To discharge that responsibility, the license holder should work closely with the CA so that they interpret security regulations properly, have clearly defined roles and responsibilities, and develop

Concept of Operations plans and other documents that the CA needs to issue licenses, such as operating licenses.

	Lifecycle Phases								
FUNDAMENTAL PRINCIPLE E: <i>Responsibility of the License Holders</i> Principle and Associated Practices	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
Principle: The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licenses or of other authorizing documents (e.g., operators or shippers).	Responsibilities assigned before Scope and Planning	X	X	X	X	X	X	X	X

4.6 Fundamental Principle F—Security Culture

All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization.

More details on this element of the physical protection regime can be found in paragraphs 3.48 to 3.51 of INFCIRC/225/Revision 5 [3]:

The **nuclear security culture** is defined as the assembly of characteristics, attitudes and behavior of individuals, organizations and institutions which serves as a means to support and enhance nuclear security. The IAEA Implementing Guide on Nuclear Security Culture, reference [15], provides an excellent discussion on this topic. There are two practices associated with this principle.

Practice Associated with this Principle: Develop and continually update a plan for developing and sustaining the security culture across the nuclear facility lifecycle using the IAEA Implementing Guide on Nuclear Security Culture.

Practice Associated with this Principle: Management should continuously monitor and enforce a positive set of behaviors.

As described in the Milestones in the Development of a National Infrastructure for Nuclear Power, IAEA Nuclear Energy Series No. NG-G-3.1 [1], a security culture that recognizes the importance of nuclear material should be in place before the State is ready to invite bids for the first nuclear power plant.

Basic tenants of security culture are that a credible threat exists and nuclear security is important. From these core beliefs should come a recognition that necessary mechanisms must be in place to plan and then finance adequate physical protection measures, including response, over the lifetime of the NPP or NF before that facility becomes operational.

More detail on this topic is included in the implementation section, under the heading Security Culture; this section provides some relevant excerpts from the Implementing Guide on Nuclear Security Culture [15].

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
FUNDAMENTAL PRINCIPLE F: <i>Security Culture</i> Principle and Associated Practices									
Principle: All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization.	Policy and program in place before Scope and Planning	X	X	X	X	X	X	X	X
Practice Associated with this Principle: Develop and continually update a plan for developing and sustaining the security culture across the nuclear facility lifecycle using IAEA Nuclear Security Series No. 7 implementing guide.	Requirements in place before Scope and Planning	X	X	X			X	X	X
Practice Associated with this Principle: Management should continuously monitor and enforce a positive set of behaviors.							X	X	X

4.7 Fundamental Principle G—*Threat*

The State’s physical protection (PP) should be based on the State’s current evaluation of the threat.

The threat is defined as “A person or group with the motivation, intention, or capability to commit a malicious act” (as defined in INFCIRC/225/Revision 5 [3]). More details on this fundamental principle of the physical protection regime can be found in paragraphs 3.34 to 3.40 of INFCIRC/225/Revision 5 [3]. It is relevant to point out that Revision 5 includes new threats not included in Rev. 4, such as cyber, airborne and standoff attacks, and includes more detail on protecting against the insider threat. It also states that a DBT should be used for Category I and high radiological consequence nuclear facilities.

The application of a design basis threat may not be necessary in low-risk facilities such as Category III facilities, where Category III refers to the IAEA material category definition. However, the need to continuously evaluate the current and potentially future-changing threat and update when appropriate remains throughout the facility lifecycle. See the IAEA Implementing Guide on the Development, Use and Maintenance of the Design Basis Threat [16].

Practice Associated with this Principle: Develop and continually update the State’s evaluation of the threat. This evaluation should be performed by the appropriate State authorities, using various credible information sources.

To evaluate the threat, trained specialists are assigned to analyze threat data and to use that data to create what is called a threat assessment; this threat assessment (TA) can be used, if the State desires, to then create what is called the Design Basis Threat or DBT. The Implementing Guide on the Design Basis Threat [16] describes the process for creating a TA and DBT. The guide suggests that a DBT be used where the consequences of a malicious act would be severe (such as theft of Category I amounts of nuclear material or high radiological consequences due to sabotage), but also where “there is too much uncertainty in the threat assessment owing to a limited amount of data or a low level of confidence in the sources of the data.” Note that there is an associated IAEA workshop on “Setting the Design Basis Threat” than can be used by a State to start development of a TA and/or DBT.

Reference [16] also states, “Regardless of whether a DBT approach or another threat based approach to security is used, the competent authority should ensure that there is a threat related basis for the resulting protection.” Thus, where a DBT is not required, some documented relationship between the protection requirements and the information collected in the TA is still needed. In this sense, the TA is never used by itself, even when there is low uncertainty in the threat assessment, due to large amounts of data from high confidence sources.

The threat assessment or DBT (if used) aid the licensing process for a NPP or NF by:

- Providing a common basis for physical protection at all facilities within the State;
- Providing a standard against which to design and evaluate a PPS, and
- Setting a baseline to evaluate future changes in the threat.

Note that the DBT differs from the TA in that the former 1) screens out those threats that lack the motivation, intention, or capability to commit a malicious act involving nuclear materials and nuclear facilities; 2) combines the information about the threat entities into a composite adversary with postulated capabilities; and 3) modifies the postulated capabilities of the composite adversary based on relevant policy considerations. While it is typically harder to create and apply a DBT, the latter serves as a State policy document that generally provides a more stable basis for security resource planning over long time horizons.

Practice Associated with this Principle: Design, measure, and validate the PPS performance against the threat. If the threat evaluation changes during the facility lifecycle, then the PPS effectiveness should be reevaluated.

The DBT/TA works as a design/evaluation standard by setting boundaries on the attacker capabilities, limiting the scenarios they can perform, and serving as a basis for conducting effectiveness evaluations of the PPS. To make use of this standard, the State and operator also need to possess the expertise to properly evaluate the effectiveness of the PPS against the DBT/TA.

More information on defining and using the DBT/TA are found in the Implementation Section under the heading Threat Assessment.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
FUNDAMENTAL PRINCIPLE G: Threat Principle and Associated Practices									
Principle: The State’s physical protection (PP) should be based on the State’s current evaluation of the threat.		X	X					X	X
Practice Associated with this Principle: Develop and continually update the State’s evaluation of the threat. This evaluation should be performed by the appropriate State authorities, using various credible information sources.	Evaluation available early in Scope and Planning phase	X	X					X	X
Practice Associated with this Principle: Design, measure, and validate the PPS performances against the threat. If the threat evaluation changes during the facility lifecycle, then the PPS effectiveness should be reevaluated.	Methodology in place before Scope and Planning	X	X				X	X	X

4.8 Fundamental Principle H—*Graded Approach*

Physical Protection (PP) requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the material and potential consequences associated with the unauthorized removal of nuclear material, and with the sabotage against nuclear material or nuclear facilities.

More information concerning the graded approach for basing PP requirements can be found in paragraphs 3.43 to 3.44 of INFCIRC/225/Revision 5 [3].

This principle focuses on the State's process for setting PP requirements based on a graded approach, but designers can take the State's graded approach into account to keep security costs as low as possible. One State-level practice is associated with this principle:

Practice Associated with this Principle: Use heuristics (e.g., category of material) or risk-informed methodologies for grading, where risk includes frequency of attack, system effectiveness, and consequence.

INFCIRC/225/Revision 5 [3] discusses the State's use of nuclear material categorization as a basis for graded security requirements for unauthorized removal of nuclear material, while the State's threshold(s) of unacceptable radiological consequences is used as a basis for graded security requirements. The latter approach ends up being risk-informed as the thresholds for unacceptable radiological consequences are based on a consequence analysis, with possible influences of the other risk components, frequency of attack and protection system effectiveness. Note that a number of risk assessment methodologies (RAMs) currently exist that could be used by the State to help link physical protection requirements to the threat, relative attractiveness of the material and or sabotage target, and the potential consequences of a malicious act.

One facility-design practice is described here, that may be usefully applied during the Scope and Planning as well as Design Concept phases of the lifecycle:

Practice Associated with this Principle: Categorize the facility and its targets in terms of material categorization for theft of nuclear material and consequences of radiological sabotage, including that caused after unauthorized removal of other radioactive material. Where there is a choice during design, keep the categorization as low as possible.

This practice suggests that the facility designer attempt to keep the target categorization level as low as possible to reduce the need for security. Examples would include use of Category III fuel versus Category I, lower source terms rather than larger ones for sabotage events, or location of reactors in areas with lower impacts on society if unacceptable releases occur. In a similar fashion, the designer might attempt to limit the size of higher category target areas, such as vital or inner areas, to keep security requirements as limited as possible. As a general rule, the designer should consider ways to reduce the consequence of an event, whether the source of the event is natural, accidental, or malicious.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
FUNDAMENTAL PRINCIPLE H: <i>Graded Approach</i> Principle and Associated Practices									
Principle: PP requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the material, and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear material or nuclear facilities.	CA developed PP requirements and graded approach before Scope and Planning	X	X					X	X
Practice Associated with this Principle: Use heuristics (e.g., category of material) or risk-informed methodologies for grading, where risk includes frequency of attack, system effectiveness, and consequence	Approach in policy before Scope and Planning	X							
Practice Associated with this Principle: Categorize facility and its targets in terms of material categorization for theft of nuclear material and consequences of radiological sabotage. Where there is a choice during design, keep the categorization as low as possible.	Methodology in place before Scope and Planning	X	X	X					

4.9 Fundamental Principle I—*Defense in Depth*

The State’s requirements for physical protection should reflect a concept of several layers and methods of protection (structural or other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives.

More details on this element of the physical protection regime can be found in paragraphs 3.45 to 3.47 of INFCIRC/225/Revision 5 [3].

INFCIRC/225 Revision 5 para.3.45 touches on several aspects of SeBD, including the importance to physical protection of the facility design: “State requirements for physical protection should be based on the concept of defense in depth for preventive and protective measures. The concept of physical protection requires a designed mixture of hardware (security devices), procedures (including the organization of guards and the performance of their duties) and facility design (including layout).” [3]

Defense in depth is a design concept in which an adversary should be required to avoid or defeat several layers and methods for physical protection in sequence. For example, an adversary might be required to defeat three security layers (limited access area, protected area, and vital area) before gaining entry to a reactor control room. Ideally, the measures used to detect, interrupt, and neutralize the adversary at these layers should be a mix of hardware (such as perimeter sensors at the limited access area and protected area boundaries); procedures (intended to search for contraband, verify identity, assess an alarm, or to shut down the reactor and secure the control room if an actual intrusion is identified); and design features (such as barrier construction and a limited number of access routes). The effect produced on the adversary by a system that provides defense in depth will be to:

- increase uncertainty about the system to the adversary,
- require additional tools and more extensive preparations prior to attacking the system, and
- create additional steps where the adversary may fail or abort the mission.

In addition, having several layers of protection provides more delay time, which increases the probability of interdiction/interruption by response forces, if different technologies are appropriately mixed and used. The chances of detection also can be increased by deploying detection elements across several layers of protection.

When dealing with the insider threat, providing defense in depth may prove difficult, especially for insiders who have direct access to nuclear material or to vital equipment. The Preventive and Protective Measures against Insider Threats Implementing Guide presents a structured method for providing defense in depth preventive and protective measures against the insider (Figure 11).

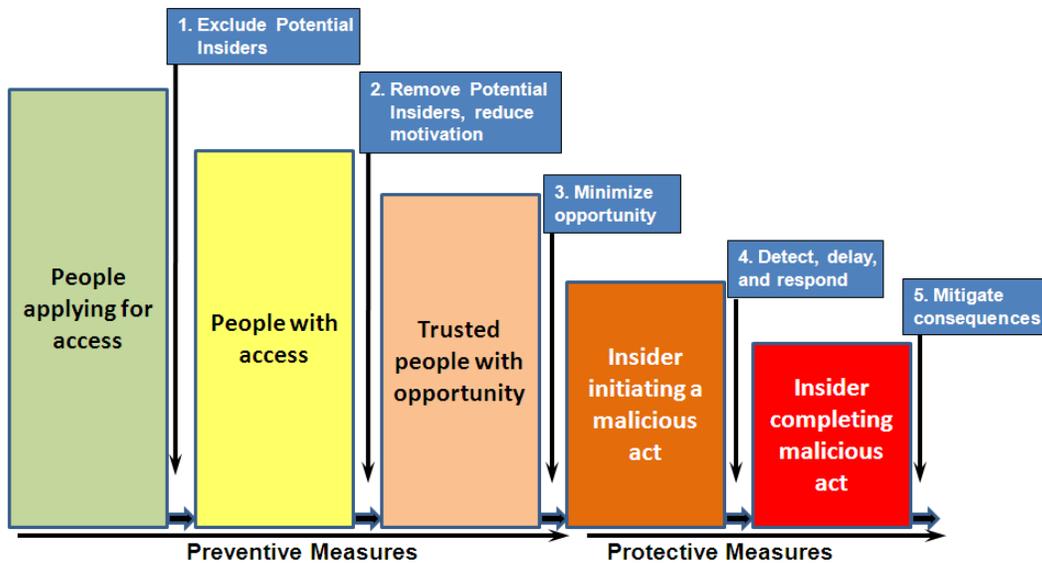


Figure 11. Defense in Depth Preventive and Protective Measures against Insiders

Practice Associated with this Principle: During the facility design, provide adequate security for elements of the physical protection system that are critical in the sense that if they fail or are defeated, PPS effectiveness will drop to unacceptable levels.

Physical protection measures contribute to timely detection (detection that occurs early enough during an adversary attack that response forces can interdict or interrupt the adversary before they complete their attack) or to neutralization (the ability to defeat the adversary, given interruption). Some of these elements—the measures themselves or the subsystems that they depend upon (such as power systems)—may be critical in the sense that if they do not work during the attack the PPS effectiveness will be unacceptably weakened. Critical elements can be identified in a general way during scoping, and can be identified more specifically as the facility design is made more detailed and the resulting evaluations of the effectiveness become more precise.

Practice Associated with this Principle: Optimize the balance of Physical Protection functions. Security system designs should seek to optimize the balance of the PPS functions of detection, delay, and response with regard to their impact on facility operations and cost commensurate with the security objectives.

Engineered controls such as access entry points should employ passive features (for example, physical barriers such as wall construction) as well as active features (for example, biometric access entry). Controls should include both administrative and engineering features, such as entry badges with both photo ID and electronic credentialing information. Note that these principles and practices apply to both software and hardware design.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
FUNDAMENTAL PRINCIPLE I: <i>Defense in Depth</i> Principle and Associated Practices									
Principle: The State’s requirements for physical protection should reflect a concept of several layers and methods of protection (structural or other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives.		X	X	X					
Practice Associated with this Principle: During the facility design, provide adequate security for elements of the physical protection system that are critical in the sense that if they fail or are defeated, PPS effectiveness will drop to unacceptable levels.			X	X					
Practice Associated with this Principle: Optimize the balance of Physical Protection functions. Security system designs should seek to optimize the balance of the PPS functions of detection, delay, and response with regard to their impact on facility operations and cost commensurate with the security objectives.			X	X					

4.10 Fundamental Principle J—*Quality Assurance*

A quality assurance policy and quality assurance programs should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied.

More details on this element of the physical protection regime can be found in paragraph 3.52 of INFCIRC/225/Revision 5 [3].

Practice Associated with this Principle: Employ formal or commonly accepted processes for quality assurance.

Practice Associated with this Principle: Ensure the PPS design is part of the larger facility quality assurance management plan.

References for ensuring the PPS design is part of the larger facility quality assurance management plan are [17], [18], [19], [20], and [21].

Practice Associated with this Principle: Use watch logs to record maintenance and operational events. Test key PPS elements.

- Logs can include such information as the number of false and nuisance alarms, component breakdowns, putting alarms in access while instituting compensatory measures. The resulting data can then be analyzed for trends.

PPS elements should be tested periodically as part of a quality assurance program, especially if such elements are key or critical (for more information on critical elements, see the previous section on Defense-in-Depth). Verify and test key PPS elements periodically.

Practice Associated with this Principle: Ensure PPS project is under Configuration Management (CM).

Helpful references on configuration management are [22, 23] (note that this reference covers both NPP design and operations), [24] and [25]. Note that the last reference covers a number of useful topics, such as examples of functional areas for configuration management requirements. Before operation, the configuration management system maintains consistency between licenses and agreements; designs; and the actual construction. During operations, a CM system maintains a record of the operational facility (including the PPS) from as-built conditions to its current status, recording modifications. The divisions that operate the facility should work closely with the groups that realize the facility so that the configuration management system for the operational facility is based on the configuration management system used during realization. Subsequent changes to the facility with the potential of substantively altering PPS performance should be evaluated formally and accepted before implementation.

Practice Associated with this Principle: Manage project requirements as they are developed during concept and realization stages (that begin at the scope and planning phase and continue until construction is complete).

Today, software systems exist that help during design (as well as operations) manage requirements as well as perform the configuration management function.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
FUNDAMENTAL PRINCIPLE J: <i>Quality Assurance</i> Principle and Associated Practices									
Principle: A quality assurance policy and quality assurance programs should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied.	CA policy and program in place before Scope and Planning		X	X	X	X	X	X	X
Practice Associated with this Principle: Employ formal or commonly accepted processes for quality assurance.			X	X	X	X	X	X	X
Practice Associated with this Principle: Ensure the PPS design is part of the larger facility quality assurance management plan.			X	X	X	X	X	X	X
Practice Associated with this Principle: Use watch logs to record maintenance and operational events. Test key PPS elements							X	X	X
Practice Associated with this Principle: Ensure PPS project is under Configuration Management (CM).				X	X	X	X	X	X
Practice Associated with this Principle: Manage project requirements as they are developed during concept and realization stages (that begin at the scope and planning phase and continue until construction is complete.			X	X	X	X			

4.11 Fundamental Principle K—*Contingency Plans*

Contingency (emergency) plans to respond to unauthorized removal of nuclear material, sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all license holders and authorities concerned.

A contingency plan is defined as a predefined set of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts.

More details on this element of the physical protection regime can be found in paragraphs 3.58 to 3.62 of INFCIRC/225/Rev. 5 [3]; note that paragraph 3.58 applies at both the State and operator levels.

Contingency (emergency) plans should be prepared and approved during the realization stage; for more explanation concerning this stage (which incorporates the design engineering, contracting and construction lifecycle activities) see section 3.3, Facility Design/Operations Lifecycle). Security contingency plans should also address non-malicious events, such as fire, flood, or wind, that result in PPS degradation and increased vulnerability.

Note that INFCIRC/225/Revision 5 [3] includes specific recommendations to locate and recover nuclear material missing or stolen from a fixed site (4.50 to 4.56 for the State and 4.57 to 4.63 for the operator) and to mitigate and minimize the consequences of sabotage at fixed sites (5.44 to 5.53 for the State and 5.54 to 5.58 for the operator). Some of these recommendations cover contingency plans.

Practice Associated with this Principle: Develop contingency plans, including response force agreements with outside agencies.

Practice Associated with this Principle: Verify response force agreements are in place. Conduct periodic scheduled and unscheduled drills and record results to evaluate facility, police, and/or military response to security events. Such drills may include measurements of time for alarm assessment, notification, and security response; and effectiveness of land-line, Radio Frequency (RF) and other communications systems.

References [26], [27], and [28] provide information about drills.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
FUNDAMENTAL PRINCIPLE K: <i>Contingency Plans</i> Principle and Associated Practices									
Principle: Contingency (emergency) plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all license holders and authorities concerned.	CA process in place before Design Engineering	X	X	X			X	X	X
Practice Associated with this Principle: Develop contingency plans, including response force agreements with outside agencies.		X	X	X					
Practice Associated with this Principle: Verify response force agreements are in place. Conduct periodic scheduled and unscheduled drills and record results to evaluate facility, police, and/or military response to security events. Such drills may include measurements of time for alarm assessment, notification, and security response; and effectiveness of communications systems (fixed, RF, etc.).	CA testing program in place before Design Engineering						X	X	X

4.12 Fundamental Principle L—Confidentiality

The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities.

More details on this element of the physical protection regime can be found in paragraphs 3.53 to 3.55 of INFCIRC/225/Revision 5 [3]. It should be noted that protection of information forms another layer of defense in depth.

Practice Associated with this Principle: PPS design, operation, and potential vulnerabilities should be handled with appropriate need-to-know control. Similarly, normal operation and contingency plans should be handled with the appropriate level of information control. This principle extends to protection of electronically transmitted information. Encryption technologies should be employed as well as use of protected networks.

FUNDAMENTAL PRINCIPLE L: <i>Confidentiality</i> Principle and Associated Practices	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/
Principle: The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities.	State policy and program in place before Scope and Planning	X	X	X	X	X	X	X	X
Practice Associated with this Principle: PPS design, operation, and potential vulnerabilities should be handled with appropriate need-to-know control. Similarly, normal operation and contingency plans should be handled with the appropriate level of information control. This principle extends to protection of electronically transmitted information. Encryption technologies should be employed as well as use of protected networks.		X	X	X	X	X	X	X	X

4.13 Other SeBD Principle—*Achieve Inherent or Intrinsic Security*

Physical protection is best realized when security objectives addressed as an intrinsic part of the facility design itself and not are added post construction as “extrinsic” features. Further, security should be included as a top-tier requirement in system design and performance that is considered at the same level as mission functionality, safety, and reliability.

Practice Associated with this Principle: Give major focus during the concept and design phases to studying facility Concept of Operations (ConOps) and designs that have reduced security needs (as in using lower Categories of material or having lower worst-case sabotage consequences), then look at strengthening facility features before addressing design of the PPS itself.

The Concept of Operations is defined and discussed in more detail in section 4.19, Other SeBD Principle—*Concept of Operations Perspective*.

While using the intrinsic security approach takes more time and effort in planning stages, the opportunities for lifecycle cost savings comes from:

- Identifying opportunities where security can be enhanced taking advantage of other features in the design or ConOps
- Resolving requirement conflicts early in the process and
- Taking a consequence-based approach that makes system assets more self-protecting and achieves PPS designs that are less threat dependent.

Properly applied, this approach can result in PPS designs that are cost-effective against both the current evaluation of the threat (see the earlier section on “Fundamental Principle G—Threat”) and are robust against potential changes in the future threat envisioned over the lifecycle of the facility (see the later section on “Other SeBD Principle—Lifecycle Perspective”).

Cost-benefit and life-cycle cost analyses can be performed to determine the trade-offs between capital costs for intrinsic security design features vs. lifetime operating costs.

	Lifecycle Phases								
Other SeBD Principle: <i>Achieve Inherent or "Intrinsic" Security</i> Principle and Associated Practices	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
Principle: Physical protection is best realized when security objectives are addressed as an intrinsic part of the facility design itself and are not added post construction as "extrinsic" features. Further, security should be included as a top-tier requirement in system design and performance that is considered at the same level as mission functionality, safety, and reliability.		X	X	X					
Practice Associated with this Principle: Give major focus during the concept and design phases to studying facility ConOps and designs that have reduced security needs (as in using lower categories of material or having lower worst-case sabotage consequences), then look at strengthening facility features before addressing design of the PPS itself.		X	X						

4.14 Other SeBD Principle—*Proven Engineering Principles*

Nuclear facilities (in general) and Physical Protection Systems (in particular) are designed, built, operated, and decommissioned using engineering practices that are proven by testing and experience, which is reflected in approved codes and standards and other appropriately documented statements.

Practice Associated with this Principle: Evaluate appropriate international standards, consider other State’s laws, and adopt applicable State laws and regulations on 3S (Safety, Safeguards, and Security) requirements and guides.

International standards, State’s laws, and State laws and regulations on 3S requirements and guides can be found in the following references: [3], [29], [30], [31], [32], and [33].

Practice Associated with this Principle: To the extent practicable, the design team should adopt commonly accepted guides and standards. When any other standard is used, the design team must demonstrate its adequacy to the regulator’s satisfaction.

The use of commonly accepted but not required standards creates a “safe harbor.” A safe harbor means the standard is understood by the regulator and meets the spirit and intent of the legal requirements.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
Other SeBD Principle: <i>Proven Engineering Principles</i> Principle and Associated Practices									
Principle: Nuclear facilities (in general) and Physical Protection Systems (in particular) are designed, built, operated, and decommissioned using engineering practices that are proven by testing and experience, which is reflected in approved codes and standards and other appropriately documented statements.	CA process in place before Design Engineering	X	X	X	X	X	X	X	X
Practice Associated with this Principle: Evaluate appropriate international standards, consider other State’s laws, and adopt applicable State laws and regulations on 3S (Safety, Safeguards, and Security) requirements and guides.				X	X	X			
Practice Associated with this Principle: To the extent practicable, the design team should adopt commonly accepted guides and standards understood by the regulator to satisfy the legal requirements. When any other standard is used, the design team must demonstrate its adequacy to the regulator’s satisfaction.				X	X				

4.15 Other SeBD Principle—*Proven Project Management Principles*

Nuclear facilities (in general) and Physical Protection Systems (in particular) are designed and built using project management practices that are proven by testing and experience, which is reflected in approved codes and standards and other appropriately documented statements. Employ formal or commonly accepted processes for project management.

Practice Associated with this Principle: Planning should allow for review, remediation, decision, and licensing. The design team should identify in the plan and scoping through licensing phases where interaction with approving authorities will occur and allow time for critical decision-making.

Part of good project management is allowing adequate time and resources for the PPT and Design and Operating Agency to interact with the State on licensing and other matters in a way that the licensing phases are successfully completed without extending the project schedule.

Practice Associated with this Principle: Implement a robust and formal project structure that includes the PP engineering with all other engineering disciplines in order to fully realize security within the entire facility design.

The PPS designers will be in a supporting role with regard to the design and construction of the NPP or NF. Therefore, the structure of the PPT's efforts should be tailored to best support these activities to ensure that security is considered throughout the process. Members of the PPT will be assigned to participate in the various activities and will be responsible for organizing and submitting input as required. For more information, see references [13] and [34].

Practice Associated with this Principle: The PPS designers should coordinate their efforts closely with other facility design teams so as to achieve seamless integration.

The approach for the PPS designers should include (1) ensuring security requirements are met by the NPPs/NFs and working with the appropriate organizations to resolve any problems, (2) identifying and resolving any security issues, (3) ensuring that the most appropriate security technologies and methodologies are adopted, (4) working with the A&E and lead organizations during all phases of the design, and (5) helping develop the technical data for, and evaluations of, alternatives.

During each of the design phases, the PPT interacts with the other facility design teams. In the conceptual design phase, the PPT helps define the threat, identify security requirements and standards, identify assets to be protected, analyze the site operating environment, and develop a basic security layout and initial PPS design descriptions. In the design-engineering phase, the system operational requirements will be defined, draft functional specifications and test/acceptance criteria will be developed, and any long-lead time purchase items will be identified; all of these activities require working with other design teams. During construction, the PPT will provide support and input to any security documents and final systems engineering testing plans, and will develop and review the facility's procedures and plans. During operations, the PPT will help integrate people, procedures, and equipment, as required.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
<p>Other SeBD Principle: <i>Proven Project Management Principles</i></p> <p>Principle and Associated Practices</p>									
<p>Principle: Nuclear facilities (in general) and Physical Protection Systems (in particular) are designed and built using project management practices that are proven by testing and experience, which is reflected in approved codes and standards and other appropriately documented statements. Employ formal or commonly accepted processes for project management.</p>		X	X	X	X	X	X	X	X
<p>Practice Associated with this Principle: Planning should allow for review, remediation, decision, and licensing. The design team should identify in the Scope and Planning through licensing phases where interaction with approving authorities will occur and allow time for critical decision-making.</p>		X	X	X	X	X	X		
<p>Practice Associated with this Principle: Implement a robust and formal project structure that includes the PP engineering with all other engineering disciplines in order to fully realize security within the entire facility design.</p>		X	X	X	X	X			
<p>Practice Associated with this Principle: The PPS designers should coordinate their efforts closely with other facility design teams to achieve seamless integration.</p>		X	X	X	X	X			

4.16 Other SeBD Principle—*Proven Operational Planning Principles*

Nuclear facilities (in general) and Physical Protection Systems (in particular) are operated and decommissioned using good planning and security practices.

Note that this document refers to the Physical Protection Team (PPT) that, during design, refers to the entity within the design team responsible for design, construction oversight, and acceptance of the PPS. During operations, the PPT refers to those responsible for the operation and maintenance of the PPS. This section refers to what is called the “security division,” that consists of the PPT during design/construction and, during operations, consists of the organizations within the NPP/NF that perform the operation and maintenance functions for the PPS under the management oversight of the PPT.

Practice Associated with this Principle: Ensure adequate staffing, funding, and independence of the security division. The necessary and sufficiently sized security division should be fully staffed and funded through the facility lifecycle and should be functionally independent from other facility functions and report directly to the facility manager.

The size, funding, and authority of the security division should be sufficient to work with the design teams in other functional areas throughout the design lifecycle. If security is to be effectively integrated into the NPP/NF, management must be willing to commit and to lead (see also the discussion in section 4.6, Fundamental Principle F—Security Culture.). As a part of this commitment, someone in the organization (i.e., senior management) must have the overall responsibility, authority, accountability, and ownership of security for the entire facility. The individual(s) assigned this responsibility should be willing and able to take on this responsibility for the long-term.

Practice Associated with this Principle: Use only trained and qualified security personnel. Consistent with quality assurance and State physical protection directives and manuals, only fully qualified personnel should have active roles consistent with their security duties. Training programs should be evaluated and updated as necessary. Personnel should undergo periodic requalification for critical skills.

In order to accomplish the successful integration of security into the design process, trained and qualified personnel need to be identified. The PPT making up the security division must be identified and assigned to participate in the process from start to finish. This PPT should consist of at least one management-level representative, one or two highly experienced and knowledgeable senior staff members, representatives from other related areas such as safety, cyber/process control, and safeguards, and operations personnel. Someone on the PPT should have experience with risk management and security assessment. The entire PPT should be provided with the opportunity to upgrade its expertise and capability through training. An example of a critical skill is use of firearms in accordance with national laws and regulations.

Practice Associated with this Principle: Verify staff trustworthiness. Sufficiently detailed background checks should be completed and results evaluated before security assignments are

made. Human reliability programs should be considered for personnel deemed by the competent authority to have “critical” access.

During the course of the security division’s activities, it is very likely that staff will gather sensitive information and, at some point, may even be required to have access to nuclear materials. For this reason, it is important that all members of the security division be properly vetted with regard to their trustworthiness and, in some cases, the level and scope of their need-to-know. Not only should background checks be performed prior to anyone being assigned to the security division, but periodic checks should be completed during the tenure of their assignment. Particular attention should be given to any past incidents that may be indicators of concern. In addition to background checks, the security organization should implement a personnel security program that not only conducts the initial and periodic checks but also may conduct security education and awareness (security culture). Depending on the situation, it may be desirable that selected personnel participate in a human reliability program. Personnel meeting such criteria might include those having access to Category I nuclear materials or vital areas.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
<p>Other SeBD Principle: <i>Proven Operational Planning Principles</i> Principle and Associated Practices</p>									
<p>Principle: Nuclear facilities (in general) and Physical Protection Systems (in particular) are operated and decommissioned using good planning and security practices.</p>			X	X			X	X	X
<p>Practice Associated with this Principle: Ensure adequate staffing, funding, and independence of the security division. The necessary and sufficiently sized security division should be fully staffed and funded through the facility lifecycle and should be functionally independent from other facility functions and report directly to the facility manager.</p>							X	X	X

	Lifecycle Phases								
Other SeBD Principle: <i>Proven Operational Planning Principles</i> Principle and Associated Practices	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
Practice Associated with this Principle: Use only trained and qualified security personnel. Consistent with quality assurance and State physical protection directives and manuals, only fully qualified personnel should have active roles consistent with their security duties. Training programs should be evaluated and updated as necessary. Personnel should undergo periodic requalification for critical skills			X	X			X	X	X
Practice Associated with this Principle: Verify staff trustworthiness. Sufficiently detailed background checks should be completed and results evaluated before security assignments are made. Human reliability programs should be considered for personnel deemed by the competent authority to have “critical” access.							X	X	X

4.17 Other SeBD Principle—*Systems Engineering Principles*

Good systems engineering techniques should be used to design and build NPPs/NFs.

Nuclear facilities (in general) and Physical Protection Systems (in particular) are both complex systems and thus are better designed and built using good systems engineering techniques.

Practice Associated with this Principle: Employ formal or commonly accepted processes for systems engineering. Review and incorporate, as desired, system engineering practices and technical guides.

Examples of systems engineering and security engineering guides are [35], [36], [37], [38], [12], [39], [40], and [41].

References [37] and [40] provide a detailed description of Systems Engineering while reference [42] is a paper that provides a general overview of the systems engineering acquisition, organizational, project; and technical processes detailed in the INCOSE Handbook [37]; see Figure 12. It should be noted that several of the elements of the SeBD approach described in this handbook, such as lifecycle planning and risk management (under risk-informed design), have corresponding processes described in the INCOSE handbook.

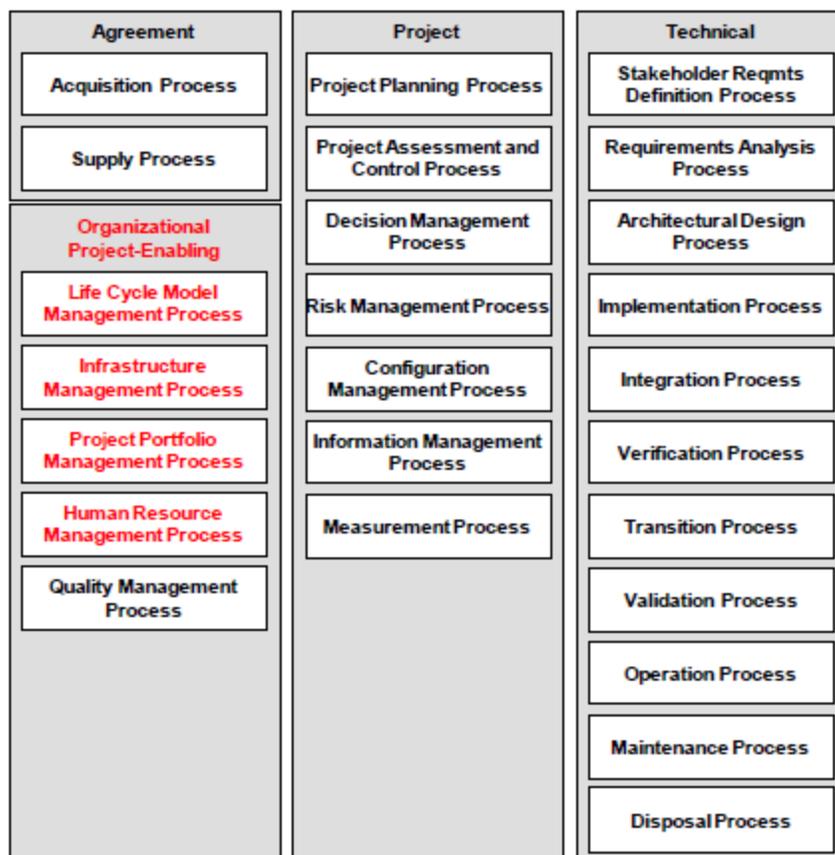


Figure 12. ISO 15288:2008 Processes

The Design and Operating Agency usually has adapted a version of systems engineering approaches, especially if the agency is an architect/engineering firm creating the NPP/NF or the vendor of the reactor. An important question is whether that adapted approach is state-of-the-art compared to the general practices found in the INCOSE Handbook, reference [37].

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/
Other SeBD Principle: <i>Systems Engineering Principles</i> and Associated Practices									
Principle: Nuclear facilities (in general) and Physical Protection Systems (in particular) are designed and built using good systems engineering principles.		X	X	X	X	X			
Practice Associated with this Principle: Employ formal or commonly accepted processes for systems engineering. Review and incorporate, as desired, system engineering practices and technical guides.			X	X	X	X			

4.18 Other SeBD Principle—*Lifecycle Perspective*

View the PPS from a lifecycle perspective. Describing the PPS design and operation in the context of its lifecycle management plan allows better requirements management from concept to sustainment.

The Facility Design/Operations lifecycle is discussed in detail in Section 3.0; note also, that a system's lifecycle perspective is also a core theme of the Systems Engineering Handbook [37]. This section serves merely to recognition of the importance of that perspective.

There are several general practices associated with this principle:

Practice Associated with this Principle: View the PPS from a lifecycle perspective during design and construction.

Practice Associated with this Principle: Define clear design requirements prior to entering the Design Concept phase: Project initiation in the realization stage must have a necessary and sufficient requirement set consistent with the facility function.

Practice Associated with this Principle: Characterize the management practices for maintenance and operations over the lifecycle based on the facility design; see ISO 15288, reference [41].

Practice Associated with this Principle: Consider possible changes in the threat during the lifecycle when designing the nuclear facility to make it more robust against future changes in the threat.

All facility lifecycle stages and operational conditions need to be analyzed for security needs and physical protection performance. This includes consideration of security during the construction phase, for example.

As much as possible, flexibility should be designed and built into the physical protection system to ensure security is preserved as conditions change over the course of the system lifecycle. Examples to consider include:

- Excess conduit and conduit channel capacity to allow addition of communications, control, and power cables for additional and/or new detection, delay, and response protection elements
- Locations where additional hardened fighting positions can be installed to address increased numbers of adversaries or capabilities
- Locations where additional active denial systems can be installed to increase delay and/or increase the potential for neutralization
- Space for expansion or additional storage.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
Other SeBD Principle: <i>Lifecycle Perspective</i> Principle and Associated Practices									
Principle: View the PPS from a lifecycle perspective. Describing the PPS design and operation in the context of its lifecycle management plan allows better requirements management from concept to sustainment.			X	X	X	X	X	X	X
Practice Associated with this Principle: View the PPS from a lifecycle perspective during design and construction			X	X	X	X			
Practice Associated with this Principle: Define clear design requirements prior to entering the Design Concept phase: Project initiation in the realization stage must have a necessary and sufficient requirement set consistent with the facility function.		X							
Practice Associated with this Principle: Characterize the management practices for maintenance and operations over the lifecycle based on the facility design (reference. ISO 15288, <i>Life Cycle Management</i>).							X	X	X
Practice Associated with this Principle: Consider possible changes in the threat during the lifecycle when designing the nuclear facility to make it more robust against future changes in the threat.	CA guidance on possible changes	X	X	X					

4.19 Other SeBD Principle—*Concept of Operations Perspective*

Achieve consistency between conceptual design and planned operations. The design team should consider the anticipated concept of operations (ConOps), including normal, emergency, and contingency operations. The PPS design should complement the ConOps.

As described in the INCOSE handbook, reference [37], the ConOps “describes the way the system works from the operator’s perspective. The ConOps includes the user description and summarizes the needs, goals, and characteristics of the system’s user community. This includes operation, maintenance, and support personnel.” The ConOps specifically identifies roles and responsibilities.

Practice Associated with this Principle: Develop a security operation and maintenance plan embodying the ConOps, and evaluate the PPS design against planned operations.

The maintenance plan should reflect planned availability of the system, based on redundancy in the design, and be consistent the operator’s sustainability plans (see section 4.21, Other SeBD Principle—Design-in Sustainability). This maintenance plan will have to be developed in coordination with the PPT as compensatory security measures will have to be in place, perhaps requiring additional guards, during planned and unplanned outages of critical PPS subsystems.

The PPS design may be evaluated against planned operations by:

- Analyzing facility security personnel roles, responsibilities, and procedures;
- Examining the impact of physical protection measures, such as entry control and contraband detection features as well as procedures for authorizing facility access;
- Evaluating PPS performance during both malicious and non-malicious abnormal events; and
- Performing modeling and simulation of the interactions between operations and security.

Such modeling and simulation can consider specific issues over the lifecycle, ranging from evaluation of access-control system congestion during the conceptual design phase to actual simulation of security operations at access-control points using operational data during the operational phase. One security simulation of value at this stage is a tabletop exercise where licensee and response organizations explore early versions of response plans looking for gaps and weaknesses.

Note that intra-site transport also needs to be considered if it occurs. Contingency plans are also important to consider during design. Designers should allow for contingencies such as power loss and routine maintenance as well as normal operations to prevent or mitigate PPS degradation.

Practice Associated with this Principle: Follow the operation and maintenance plan during the operational phase of the facility lifecycle. The ConOps developed during design and construction phases should be followed and evaluated periodically to see if it is still current, and the operation and maintenance plan should be revised if necessary.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
<p align="center">Other SeBD Principle: <i>Concept of Operations Perspective</i> Principle and Associated Practices</p>									
<p>Principle: Achieve consistency between conceptual design and planned operations. The design team should consider the anticipated concept of operations (ConOps), including normal, emergency, and contingency operations. The PPS design should complement the ConOps.</p>			X	X			X	X	
<p>Practice Associated with this Principle: Develop a Security operation and maintenance plan embodying the ConOps, and evaluate the PPS design against planned operations.</p>			X	X					
<p>Practice Associated with this Principle: Follow the operation and maintenance plan during the operational phase of the facility lifecycle. The ConOps developed during design and construction phases should be followed, evaluated periodically to see if it is still current, and the operation and maintenance plan revised if necessary.</p>							X	X	

4.20 Other SeBD Principle—*Synergy between Safety, Safeguards, and Security*

Balance safety, domestic safeguards, and security in the design, looking for opportunities to gain synergy with complementary requirements across these functions. Safety, Safeguards, and Security should be properly integrated across the facility lifecycle, as the PPS must function in concert with safety and safeguards requirements.

A reference on this topic is [39].

Practice Associated with this Principle: The safety, domestic safeguards, and security requirements should use technically sound methods to prioritize, resolve potential conflicts between safety, domestic safeguards, and security functions, and then state results as system design requirements. The design team must resolve any conflicts that occur between safety and security.

Practice Associated with this Principle: Employ trade-off studies to explore synergy between safety, domestic safeguards, security, and operations over the set of feasible planning options during a particular project phase. These studies should be sufficiently broad to control the risk of missing an important option and should include the correct experts so that the trade-off studies are performed correctly, with the correct data and methods.

Note that studies can be performed early in the lifecycle to consider trade-offs between requirements, such as regulations, and design and operational costs, allowing the competent authority some rationale on reducing or waiving some of the regulations. Later in the design process, modeling and simulation of facility operations helps show the trade-offs between operations and security costs, for example.

Practice Associated with this Principle: Continuously compare the PPS design features with facility safety and safeguards features for both synergies and conflicts. Determine the resolution process and establish design priorities among safety, domestic safeguards, and security features to resolve conflicts as they may occur.

During design, it is useful to create crosswalk tables to compare security features with safety and safeguards requirements and features; such tables would be similar in concept to those used in reference [9] to integrate safety into the facility design.

Practice Associated with this Principle: Use guides and standards to aid in the integration of safety, domestic safeguards, and security.

It is important to realize that the security design process is performed within a larger regulatory framework that also considers safety and safeguards – the “3S” process. The following guides and standards assist in integrating these three functions: References [9], [11], and [33] and [39], while reference [43] is an excellent reference on 3S. Much more work needs to be done on developing tools, strategies, and practices for integrating safety, security and safeguards requirements properly into the overall facility design process, as well as demonstrating that the integrated design process does improve overall effectiveness and reduces lifecycle costs of the overall facility design.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
<p align="center">Other SeBD Principle: <i>Synergy between Safety, Safeguards, and Security</i> Principle and Associated Practices</p>									
<p>Principle: Look for opportunities to gain synergy with complementary requirements across the safety, security, and safeguards functions: Safety, Safeguards, and Security should be properly integrated across the facility lifecycle, as the PPS must function in concert with safety and safeguards requirements.</p>		X	X	X	X	X			
<p>Practice Associated with this Principle: Employ trade-off studies to explore synergy between safety, safeguards, security, and operations over the set of feasible planning options during a particular project phase. These studies should be sufficiently broad to control the risk of missing an important option and should include the correct experts so that the trade-off studies are performed correctly, with the correct data and methods.</p>		X	X						
<p>Practice Associated with this Principle: The safety and security requirements should use technically sound methods to prioritize, resolve potential conflicts between safety and security functions, and then state results as system design requirements.</p>				X	X				
<p>Practice Associated with this Principle: Continuously compare the PPS design features with facility safety and safeguards features for both synergies and conflicts. Determine the resolution process among safety, safeguards, and security features to resolve requirements conflicts as they may occur.</p>			X	X	X	X			
<p>Practice Associated with this Principle: Use guides and standards to aid in the integration of safety, safeguards, and security.</p>		X	X	X	X	X			

4.21 Other SeBD Principle—*Design-in Sustainability*

Designs should consider the operations phase and future activities required to maintain, test, repair, and upgrade the PPS throughout the entirety of its lifecycle. Such actions include logistics, planned maintenance, and unscheduled maintenance.

More details on this sub-element of the physical protection regime can be found in paragraphs 3.56 to 3.57 of INFCIRC/225/Revision 5 [3].

Practice Associated with this Principle: The State should establish a sustainability program to ensure its physical protection regime is sustained and effective in the long term by committing the necessary resources.

Practice Associated with this Principle: Develop the operational sustainability plan using the PPS design characteristics.

It should be emphasized that all aspects of the facility design should be under a sustainability program, including configuration management, so that a stand-alone PPS sustainability program should not be needed except in special circumstances. An operational sustainability plan should be developed during the design and construction phases, based on the PPS design characteristics. A number of activities, listed here, would provide the basis for that plan:

- Evaluate components for anticipated lifecycle, and plan for replacement or repair.
- Assure that the PPS effectiveness does not degrade unacceptably during either planned or unplanned maintenance.
- Develop a logistics plan for PPS component replacement and scheduled upgrades.
- Define a maintenance plan and integrate with facility lifecycle to include periodic maintenance assessments.
- Examine needs for trained and qualified PPS maintenance and operations personnel.
- Define testing and calibration needs for certain novel PPS components (for example, 3D video motion detection).

Practice Associated with this Principle: Implement and follow the operational sustainment plan.

Part of implementation is a trend analysis of equipment performance records and operational assessments based on ConOps performance and exercises. The plans may need to be updated based on any PPS upgrades in response to changed threat basis or observed PPS deficiencies and degradation over time. Adherence to this plan is essential for the continued assurance of PPS reliability, full functionality, and minimization of premature component failure.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
Other SeBD Principle: <i>Design-in Sustainability</i> Principle and Associated Practices									
Principle: Designs should consider the operations phase and future activities required to maintain, test, repair, and upgrade the PPS throughout the entirety of its lifecycle. Such actions include logistics, planned maintenance, and unscheduled maintenance.			X	X	X	X	X	X	X
Practice Associated with this Principle: The State should establish a sustainability program to ensure its physical protection regime is sustained and effective in the long term by committing the necessary resources.	Program in place before Scope and Planning								
Practice Associated with this Principle: Develop the operational sustainability plan using the PPS design characteristics.			X	X	X	X			
Practice Associated with this Principle: Implement and follow the operational sustainment plan.							X	X	X

4.22 Other SeBD Principle—*Balance Prescriptive and Performance-Based Requirements*

To the extent practicable, the design team should ensure appropriate balance between prescriptive and performance-based requirements through grading or compliance relief in cooperation with the Competent Authority to achieve an efficient and effective PPS.

Practice Associated with this Principle: As much as possible, maintain a close and honest working relationship with the competent authority during all phases. While this relationship must respect the competent authority’s independence, the intent should be to ensure effective communications and collaboration so that issues, such as the balance between various types of requirements, are anticipated and addressed quickly and efficiently.

The Design and Operating Agency, as well as the PPT, do not set requirements promulgated by the CA. At the same time, during requirements analysis, either of these teams may discover requirements that have significant impact on security, other functions, or cost without providing much value. The design team may then enter into discussions with the CA to see if the relative importance of some of the requirements can be adjusted or “rebalanced.” The IAEA document Facility Design and Plant Operation Features that Facilitate the Implementation of IAEA Safeguards, reference [8], covers safeguards rather than security, but does discuss the need for the IAEA and the facility designer to work more closely together, for example.

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
Other SeBD Principle: <i>Balance Prescriptive and Performance-Based Requirements</i> Principle and Associated Practices									
Principle: To the extent practicable, the design team should ensure appropriate balance of both through grading or compliance relief in cooperation with the competent authority to achieve an efficient and effective PPS.		X	X	X	X				
Practice Associated with this Principle: As much as possible, maintain a close and honest working relationship with the competent authority during all design phases. While this relationship must respect the competent authority’s independence, the intent should be to ensure effective communications and collaboration so that issues are anticipated and addressed quickly and efficiently.		X	X	X	X				

4.23 Other SeBD Principle—*Validate Effective Communication and/or Operational Agreements with Other Agencies*

The facility security organization should maintain good communications with other agencies such as police or military and have up-to-date and effective operational agreements or Memorandums-of-Understanding.

Practice Associated with this Principle: As mutually agreed, the site should conduct planned and unplanned exercises to verify that effectiveness of communications and emergency response.

INFCIRC/225/Revision 5 [3] has specific recommended requirements concerning such agreements and exercises, such as paragraphs 4.54-4.55 for addressing missing or stolen nuclear material from fixed sites

	Lifecycle Phases								
	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
<p>Other SeBD Principle: <i>Validate Effective Communication and/or Operational Agreements with Other Agencies</i></p> <p>Principle and Associated Practices</p>									
<p>Principle: The facility security organization should maintain good communications with other agencies such as police or military.</p>	CA responsible for coordination						X	X	X
<p>Practice Associated with this Principle: As mutually agreed, the site should conduct planned and unplanned exercises to verify that effectiveness of communications and operational agreements.</p>							X	X	X

4.24 Other SeBD Principle—*Project and Operations Experience*

Organizations concerned ensure that design, construction, and operating experience relevant to security are exchanged, reviewed, and analyzed, and that lessons are learned and acted on. This process will be carried out within the confidentiality requirements established by the State.

Practice Associated with this Principle: Lessons learned—both good and bad—from current and completed projects should be evaluated and disseminated. The project team should record all important lessons learned as these are identified. When no previous documentation exists, the design team should consult with earlier design teams and collect their best practices. Note that lessons learned can also be adopted based on similar experience in other countries, for example, on the use of similar nuclear facility designs.

The lessons learned from other countries may come through the competent authority with the assistance of the IAEA or may be passed through the design and/or construction organization; some may also come through the vendor of the reactor, for example.

A number of international institutions fill this role for the nuclear security community:

- The World Institute for Nuclear Security in Vienna, Austria, that periodically has conferences covering important topical areas in nuclear security and then releases best-practice guides.
- The Institute of Nuclear Materials Management (INMM) that has an important conference once a year in the United States, publishes a journal, and has chapters all over the world.

		Lifecycle Phases							
Other SeBD Principle: <i>Project and Operations Experience</i> Principles and Associated Practices	Assumptions	Scope and Planning	Design Concept	Design Engineering	Contracting	Construction	License to Operate	Operational Phase	Decommissioning/ Dismantlement
		<p>Principle: Organizations concerned ensure that design, construction, and operating experience relevant to security are exchanged, reviewed and analyzed, and that lessons are learned and acted on. This process will be carried out within the confidentiality requirements established by the State.</p>	CA responsible for organizing these programs	X	X	X	X	X	X
<p>Practice Associated with this Principle: Lessons learned—both good and bad—from current and completed projects should be evaluated and disseminated. The project team should record all important lessons learned as these are identified. When no previous documentation exists, the design team should consult with earlier design teams and collect their best practices. Note that lessons learned can also be adopted based on similar experience in other countries, for example, on the use of similar nuclear facility designs.</p>		X	X	X	X	X	X	X	X

5 Detailed Application of the Principles and Practices

Based on similar experience with Safety by Design, it is clear that early identification of physical protection requirements and intrinsic features will benefit the design [10]. In the security realm, the closest open-source descriptions of SeBD processes are found in prison design and construction. For example, in the United States, the Minnesota Department of Corrections designed and built a Level 5 maximum-security prison at Oak Park Heights [44]. The design for this facility had security of the prisoners, the staff, and the public as a critical design features. The staff and management of Minnesota's maximum-security prison at Stillwater were stakeholders in the design and had a heavy influence on the design. The result of this approach is a prison has never had a homicide or an escape since it opened in 1982, even though the prison houses prisoners requiring maximum security and one of the nine living units houses offenders who have a history of assaulting prison staff or attempting to kill other inmates.

The rest of this section begins with a discussion of specific practices that competent authorities can take to encourage the application of SeBD on the one hand and that designers can take to help implement SeBD at the Facility layout Level. We have also included a section on how adversary capabilities might change in the future and possible countermeasures that designers can employ now to be ready for those changes; this is provided to give some general guidance to designers on how to protect against such trends, against the possibility that those trends may materialize in future DBTs/TAs.

5.1 Competent Authority Practices That Support SeBD

This section describes several specific practices that competent authorities can take to encourage the use of SeBD. Several of these practices have been learned the hard way over the last 25-30 years, while others are based on good approaches in oversight and licensing. Based on this experience, the CA should consider:

1. Keeping the long lifetime of nuclear facilities in mind when creating regulations and licensing processes, and developing either DBT or threat assessment (TA) approaches to protection. This practice suggests that the CA encourage licensees to plan for future increases in the DBT/TA (some of the areas where the DBT/TA may increase are described below), as well as requiring CA approval of sustainability plans, among other things indicating how security will be funded over the life of the plant. Funding bottlenecks during the facility lifecycle can severely limit system effectiveness, either whether they are caused by funding cuts or increases in the DBT/TA or both.
2. Realistically determining whether the concept for response forces is both effective and fits well within societal norms for that particular country. In some countries, societal norms are comfortable with allowing onsite response forces capable of defeating the adversary, while other countries are more sensitive to the appearance of military-like forces stationed at their nuclear facilities. In the latter case, the legal and regulatory framework, as well as the CA, may either allow minimal armed holding forces on site or, in the extreme, no armed response

capability on site. In either case, a simple calculation for an approximate value of Probability of Interruption, P_i , will help determine whether delay time found within a facility adequately exceeds the Physical Protection System Response Time (PPSRT) provided by the approach for providing response forces.

It should also be noted that response forces arriving from offsite must contend with protection on response routes and may need to attack an adversary force that has already taken control of the site. Ideally, response force training and weapons should at least match adversary capabilities as defined in the DBT/TA.

3. Embedding security by design principles and practices within the process for licensing the construction and operations of new facilities. Even with performance-based requirements in legal and regulatory regimes, organizations constructing new facilities will tend to fall back on historical practices of hiring security consultants, treating security as one more requirement, performing the minimal effort needed to meet performance-based security requirements for an existing DBT/TA, and designing the security system as a subsystem at a point where operations, safety, and the facility layout has been largely determined. The CA is encouraged to take a more proactive approach, where the organization designing and constructing the facility is asked to a) demonstrate how they have incorporated security as a basic requirement, on the same level of importance as operations, safeguards, and safety, early in the organization of design activities as well as their design process; b) show how they have taken advantage of inherent or intrinsic features of the facility and site to improve security, to include layout and operations, as well as safety systems and security culture; c) and describe, in plans created during conceptual design, how their facility design will allow response forces, both security and emergency response, to properly plan and adequately protect the site and mitigate consequences of an attack. If nothing else, it may be useful to ask them to show how they have implemented the principles and practices found in this handbook.
4. Enforcing a performance-based physical protection regime with exercises and assessments, through adequate funding or regulatory requirements. Based on the recommendations in INFCIRC/225/Revision 5 [3], CAs are encouraged to require performance testing of physical protection regimes, systems, and measures. The basic tools for such testing, such as test protocols, vulnerability analysis methods and procedures, and templates for interagency exercise agreements and plans, already exist in readily usable form and training courses on all of these topics are available. Response time tests for offsite forces at both planned and existing facilities, as well as joint exercises at existing facilities can also be required by the State's legal and regulatory framework.

5.2 Implementing Security by Design at the Facility Level

Some general comments will be made here about how to apply SeBD to new or existing facility designs, taking into consideration design options for facilities processes or reactor designs, and associated facility layouts and adjacencies when one of the primary concerns is protecting radiological and/or nuclear

material from theft or sabotage. Note that this enlarges on the “Establish Facility Design Options” phase of the Design and Evaluation Process in Figure 4 of Section 3.2, Risk-Informed Design.

The main security concerns for radiological and/or nuclear material at a facility are that an adversary may disperse that material onsite or offsite and/or may steal it with the intent to create a nuclear explosive device, respectively. One way to develop the facility design in conjunction with development of the PPS is to follow a four-step approach, iteratively:

1. Early in the design process, consider the facility mission and operational needs, set the facility operations requirements, determine security grading, and design the operational processes to reduce the amount of material and its categorization (for theft) or minimize the level of radiological consequences (for dispersal or sabotage), and to make security response, material recovery, or dispersal incident mitigation easier. A preliminary theft and target analysis can be performed to determine where protection is required in the operations or processes. This is also a phase where siting criteria can be examined to determine if some operations or processes will be better for some sites than others. Mathematical models and simulations of processes help tradeoff analysis in this phase.
2. Based on the options for operations and processes, design the plant layout, taking into account where targets⁵ are located, where the security areas (such as protected area and inner/vital areas) will be defined, how access control and contraband control will be performed within the security area structure, what the Material Balance Areas and measurement points will be, where people and/or material movements will be tracked, and how containment and surveillance will be implemented. Physical protection plans for special operating states, such as emergency conditions, need to be developed to help determine whether safe havens will be used and where emergency exits will be located. This is also an important phase to start looking at categorization of potential insiders and schemes to compartmentalize the facility to limit the number of personnel in areas near targets, while also considering how this limitation will negatively affect operations. Timely detection analysis, based on Adversary Sequence Diagrams (ASD's) organized around security areas, and simulations of operations and security measures support design at this phase.
3. Based on operations, processes, and plant layout, determine equipment requirements for physical protection, material control and accountability, material and personnel tracking, and operational process monitoring. At this phase, response and training plans are developed and reviewed. During this phase, best practices are applied to address future needs (for example, leaving extra room in cable chases for future growth). Timely detection analysis, based on ASDs organized around the facility physical layout, and simulations of security effectiveness for both outsider and insider threats support design at this phase.

⁵ Targets include theft and sabotage targets as well as critical PPS elements, such as alarm stations and important alarm communications and entry control lines.

- Based on operations, processes, and plant layout, and equipment requirements, design the specific PPS equipment, procedures, and training. Similar analysis and simulations are used at this phase as in phase 3, although the level of detail is more advanced during this phase.

Note that the first two steps match conceptual design phases for normal process facilities; for SeBD, security considerations are factored into these design phases.

It should be recognized that these four steps can be applied either to a new facility design or to a security upgrade at an existing facility. The only difference is that modifications to processes, operations, and layouts are typically more constrained in upgrades than new facility design.

Figure 13 and Figure 14 below depict some of the considerations during steps 1 and 2 of this four-step approach. Figure 13 shows how several activities in the SeBD Design and Evaluation Process can be linked together to better reduce protection requirements related to theft of material and or sabotage considerations. In the requirements step, where PPS objectives are being determined, the facility mission and related targets can be analyzed to look at tradeoffs in terms of vital area/inner area requirements. During the Facility Design Options step, these considerations can be addressed again with process/reactor design options as well as facility layout options in mind. Both emergency response and security response needs can be considered during both of these steps.

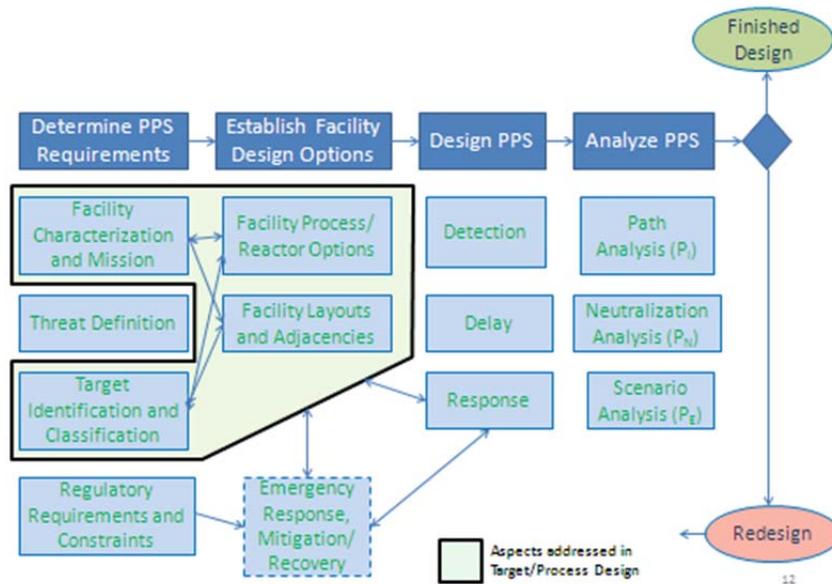


Figure 13. Target, Facility Design, and Response Analysis

Figure 14 depicts part of the second step where the plant layout is designed taking into account where targets are located, where personnel and material flow through the facility, and how the security areas (e.g., Protected Area) are mapped into the layout. Several security-related factors, such as entry and exit control, containment/surveillance, and area access for insider protection, can be considered.

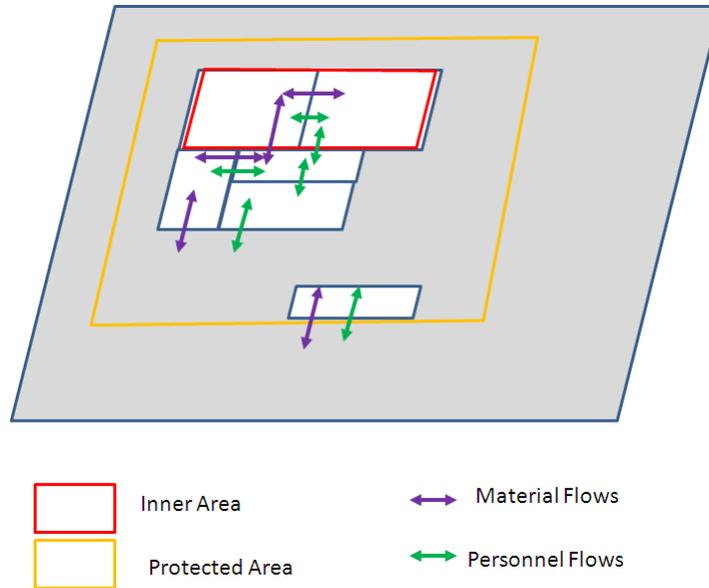


Figure 14. Layout versus Personnel/Material Flows and Security Areas

5.3 Possible Areas Where the DBT/TA Capability May Increase in the Future

It is difficult to predict what future changes may occur in the threat, in terms of motivation, objectives, and capability. At the same time, certain trends have occurred over the last 30 years, which may continue in the future, as shown in Table 4, along with possible security by design countermeasures.

As stated earlier, providing the PPT with information on the risks identified in addition to the risk informed decision, allows the PPT to make design decisions based on the identified threat when economically feasible. In other words, limiting the information the PPT has from the State or the CA limits the PPT’s ability to address and control risk. Allowing the PPT to understand the potential for the future threat will allow consideration of cost-effective design features inherently. This does not mean that the PPT will meet the potential increase in the threat, just that the design will be easier to adapt.

Other areas that the PPT should address during selection of physical protection measures are reliability and availability. These areas are typically worked with vendors. For example, how long will Microsoft support certain operating systems? Will the electronic systems be upwardly compatible? How easily is the network bandwidth expanded (for example, expansion of video systems to handle digital communications)?

Table 4. Threat Capabilities That Might Change over Time and Possible Design Countermeasures

Topic	Possible Countermeasures
Hypothetical changes in capabilities to any threat attempting to commit	
<ul style="list-style-type: none"> • Sabotage 	Reduce number of vital areas subject to sabotage, build on safety concepts such as inherently safe designs, and locate them so that they are easier to protect.
<ul style="list-style-type: none"> • Theft 	Reduce the number and inventory of Inner Areas with Category I material, and locate them to so that they are easier to protect.
Hypothetical changes to External Threats	
<ul style="list-style-type: none"> • Better attack vehicles 	Room for more standoff and improved and possibly more vehicle barriers; early detection capabilities against unauthorized vehicles
<ul style="list-style-type: none"> • Lighter and/or more capable tools and more capable explosive attacks 	Provide thicker walls, allow room for more doors and/or activated delays, and design “nested” security layers, with no common walls across multiple layers
<ul style="list-style-type: none"> • Better weapons and/or weapons training 	More capable weapons and training as well as use of fighting positions with overlapping fields of fire, hardened facility post and hardened response vehicles for more survivability
<ul style="list-style-type: none"> • More adversaries and/or better tactics 	Allow for a larger protective force and/or better tactical training
<ul style="list-style-type: none"> • Increased frequency of or capability of unarmed antinuclear activists 	Improved site features and security plans, as well as regulatory changes, to make it easier for guards to prevent the entry of and to arrest such activists
<ul style="list-style-type: none"> • Cyber-attack capabilities 	Better cyber protection, both for control systems and critical security systems
Hypothetical Changes to Internal Threats	
<ul style="list-style-type: none"> • More active and or violent insider adversaries; or multiple insiders 	Compartmentalize layout and limit those with access, authority, and knowledge of security systems and targets. Track human and material movement.
<ul style="list-style-type: none"> • Cyber-attack capabilities 	Better cyber protection, both for control systems and critical security systems

6 Summary

This handbook describes an approach to Security by Design (SeBD), to familiarize readers with SeBD, and to provide some principles and practices, as well as practical insights, on how to implement and achieve SeBD. The handbook is aimed at decision makers, advisers, and senior managers in governmental organizations, utilities, industries, and regulatory bodies of a country interested in developing nuclear power.

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, to include construction and 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.

The approach to SeBD is explained within the context of the framework of milestones in the development of a national nuclear infrastructure (see references [1,2]) 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) [3]. 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.

Some key elements of a SeBD approach are the use of: an Integrated Design Team to coordinate design teams covering multiple domains of expertise; risk informed design to address threat, vulnerability and consequences within a holistic framework; a structured process for considering the lifecycle of the facility; and employing a number of SeBD principles and practices. Another useful design practice is to consider security features that are intrinsic to the facility design, rather than considering security after the facility has entered detailed design during the design-engineering phase. Equally important is a robust nuclear security culture, active quality and configuration management systems, and a recurring assessment of the PPS performance with respect to the current DBT.

An earlier draft of this handbook included information to support the Work Plan of the Nuclear Security Summit to share best practices for nuclear security in new facility design. This Work Plan called on States to "encourage nuclear operators and architect/engineering firms to take into account and incorporate, where appropriate, effective measures of physical protection and security culture into the planning, construction, and operation of civilian nuclear facilities and provide technical assistance, upon request, to other States in doing so." The production of this preliminary draft is a step in the Japan-US Joint Nuclear Energy collaboration conducted under the Project Action Sheet, PAS-PP04, between the United States Department of Energy (DOE) and the Japan Atomic Energy Agency (JAEA).

References

1. 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.
2. International Atomic Energy Agency, *Evaluation of the Status of National Nuclear Infrastructure Development*, Nuclear Energy Series, No. NG-T-3.2, Vienna, 2008.
3. 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.
4. International Atomic Energy Agency, *Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual – Physical Protection, Volume 6 of the Final Report of Phase 1 of the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO)*, IAEA-TECDOC-1575, Vienna, 2008.
5. International Atomic Energy Agency, *Basic infrastructure for a nuclear power project*, IAEA-TECDOC-1513, Vienna, June 2006.
6. The Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group of the Generation IV International Forum, *Addendum to the Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems, Technical Addendum to Revision 5*, (January 31, 2007).
7. International Atomic Energy Agency, *Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1 INSAG-12 A Report by the International Nuclear Safety Advisory Group*, 1999
8. *Facility Design and Plant Operation Features that Facilitate the Implementation of IAEA Safeguards SGCP-CCA*, February 2009, IAEA Department of Safeguards, STR-360.
9. DOE-STD-1189-2008, *Integration of Safety into the Design Process 2008*, US Department of Energy.
10. *Review and Analysis of Development of “Safety by Design” Requirements*, J. Hockert, SA Vance, October 2009, Pacific Northwest National Laboratory, PNNL-18848.
11. *Integrating Safeguards and Security with Safety into Design*, Robert S. Bean, John W. Hockert, and David J. Hebditch, May 2009, INL/CON-09-15887 Idaho National Laboratory, presented at the 19th Annual EFCOG Safety Analysis Workshop.
12. Garcia, Mary Lynn, *Vulnerability Assessment of Physical Protection Systems*. Burlington, MA: Elsevier Butterworth-Heinemann, 2006.
13. Project Management Institute, *Project Manager Body of Knowledge*, (December 2008).
14. *Nuclear Power Plant Design*, course PD 609 June 2010, American Society of Mechanical Engineers.
15. International Atomic Energy Agency, *Implementing Guide for Nuclear Security Culture*, Nuclear Security Series No. 7, Vienna, 2008.
16. International Atomic Energy Agency, *Implementing Guide, Development, Use and Maintenance of the Design Basis Threat*, Nuclear Security Series No. 10, 2009.
17. International Standards Organization (ISO) 9000, *Quality Management Systems*, 2008.
18. *Japan Quality Management System*.
19. DOE Order 414.1C, *Quality Assurance*.
20. US Code of Federal Regulations 10 CFR 830.
21. American Society of Mechanical Engineers (ASME), NQA-1-2004, *Nuclear Quality Assurance*.
22. International Standards Organization (ISO), ISO 10007, *Configuration Management*, 2003.

23. International Atomic Energy Agency, Configuration management in nuclear power plants, IAEA-TECDOC-1335 (IAEA, 2003).
24. Information Technology Impact on Nuclear Power Plant Documentation, IAEA-TECDOC-1284 (IAEA, 2002).
25. Information Technology for Nuclear Power Plant Configuration Management, IAEA-TECDOC-1651 (IAEA, 2010).
26. DOE Manual 470.4.
27. Japan Ministry of Economy, Trade, and Industry Training Manual (controlled).
28. Japan Ministry of Education, Culture, Sports, Science, and Technology Training Manual (controlled).
29. Japan Act Number 166 (Act on the Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactor), 2002.
30. International Atomic Energy Agency, *The Convention on the Physical Protection of Nuclear Material*, INFCIRC/274/Rev.1.
31. International Atomic Energy Agency, *Code of Conduct on the Safety and Security of Radioactive Sources*, Vienna, 2004.
32. US Code of Federal Regulations 10 CFR 73.
33. US DOE, DOE P 470.1, Integrated Safeguards and Security Assessment (ISSM) Policy.
34. DOE Order 413.3A, Project Management for the Acquisition of Capital Assets.
35. D. W. Whitehead, C. S. Potter, S. L. O'Connor, *Nuclear Power Plant Security Assessment Technical Manual*, SAND2007-5591, Sandia National Laboratories, September 2007.
36. International Atomic Energy Agency -Technical Document (TECDOC)-967 (Rev.1), *Guidance and Considerations for the Implementation of INFCIRC/225/Rev.4*, Vienna, 2000.
37. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, Version 3.2.2, October, 2011, International Council on Systems Engineering (INCOSE).
38. Garcia, Mary Lynn, *The Design and Evaluation of Physical Protection Systems*. Woburn, MA: Butterworth-Heinemann, 2001.
39. Idaho National Laboratories, Institutionalizing Safeguards-by-Design Handbook: High Level Framework.
40. Systems Engineering Fundamentals, January 2001, Department of Defense Systems Management College.
41. ISO 15288, Systems and software engineering – System life cycle processes, March 18, 2008, International Organization for Standardization.
42. INCOSE Systems Engineering Handbook v3.2: Improving the Process for SE Practitioners, 2010, R. Douglas Hamelin, David D. Walden, Michael E. Krueger, Battelle Energy Alliance, LLC.
43. IAEA-CN-184/64, *Investigating 3S Synergies to Support Infrastructure Development and Risk-Informed Methodologies for 3S by Design*, M. Suzuki, Y. Izumi, T. Kimoto, Y. Naoi, T. Inoue, B. Hoffheins, Nuclear Nonproliferation Science and Technology Center, Japan Atomic Energy Agency.
44. Wikipedia article dated November 6, 2012 at [http://en.wikipedia.org/wiki/Minnesota Correctional Facility %E2%80%93 Oak Park Heights](http://en.wikipedia.org/wiki/Minnesota_Correctional_Facility_%E2%80%93_Oak_Park_Heights)

45. R. V. Matalucci, D. S. Miyoshi, S. L. O'Connor, *An Introduction to Architectural SuretySM Education*, SAND98-2086, Sandia National Laboratories, September 1998.
46. DOE G 413.3-17, *Mission Need Statement Guide*, June 20, 2008.
47. International Atomic Energy Agency, *Handbook on the Physical Protection of Nuclear Facilities*, IAEA-Tecdoc-1276, Vienna, March 2002.
48. Sandia National Laboratories, *International Training Course 22*, SAND 2010-6008P, Sandia National Laboratories, October 2010.
49. Institute for Nuclear Materials Management, *Global Best Practices for Physical Protection*, Special International Workshop on Global Best Practices in Physical Protection, June 14-18, 2004, Prague, Czech Republic.
50. International Atomic Energy Agency, *Preventive and Protective Measures against Insider Threats*, Nuclear Security Series No. 8 Implementing Guide, Vienna, 2008.
51. Department of Energy (DOE) M 470-2, *Physical Protection Manual*.
52. IAEA Nuclear Security Series No.11, Implementing Guide, Security of Radioactive Sources, 2009.
53. US Nuclear Regulatory Commission, *Vital Equipment/Area Guidelines Study: Vital Area Committee Report*, NUREG-1178, Washington, D.C., February 1988.
54. International Atomic Energy Agency, *Safety of Nuclear Power Plants: Design*, Safety Standards Series No. NS-R-1, Vienna, 2000.
55. US Code of Federal Regulations 10 CFR 100.
56. Lessler, R. M., and A. S. Ahluwalia, "Safeguards assessment of spent fuel disposal alternatives," Proceedings of the 20th Annual Meeting of the Institute of Nuclear Materials Management, Journal of the Institute of Nuclear Materials Management, Vol. VIII, Proceedings Issue, pp. 790-806, 1979.
57. US Code of Federal Regulations 10 CFR 50.
58. Cipiti, B.G., and F.A. Duran, *Integrated Safeguard and Security for Material Protection, Accounting and Control*, SAND2009-6781, Sandia National Laboratories, Albuquerque, New Mexico, October 2009.

Appendix A – Security by Design Generic Design Process

This appendix describes the essential notional lifecycle actions to achieve Security-by-Design by the three key entities: State, Design and Operating Agency, and Physical Protection Team. Placing them in side-by-side columns allows comparison of relative time, precedence, and dependencies. The authors did not attempt to define decision makers or to define timelines. Definitions of these would occur when needed and are highly conditional on factors well outside the scope of this document. Note that the project team is portrayed in this document as being an entity within the Design and Operating Agency.

A.1 Scope and Planning Phase

Several pre-project activities commence following the State's intent to implement nuclear power. Normally these actions, which are described in the IAEA *Milestones in the Development of a National Infrastructure for Nuclear Power* [1], should occur before NPP/NF project initiation. Critical actions with respect to project initiation are defined by the legal, regulatory, and environmental criteria associated with NPP/NF construction, operation, and dismantlement.

The IAEA recommends that the State form a NEPIO. Initially, the NEPIO is the pre-project team to examine the high-level requirements (the “what's”) and determine the feasibility of the project. Considerations would be the capacity/capability of the NPP/NF, the potential sites for the NPP/NF, the infrastructure needs beyond existing, anticipated construction costs, and so on. The State's threat assessment or published DBT provides the basis for determining the physical protection objectives. Based on these considerations, this pre-project team should develop a Scope and Planning document describing the high-level operational concept and the related factors allowing grading by the NPP/NF project team.

Grading is the State's determination of the necessary set of 3S requirements for the NPP/NF acceptance and operation. The IAEA implementation guide to INFCIRC/225/Rev. 4 [36] provides guidance on PPS grading for theft and sabotage.

The NPP/NF site location may impose additional security constraints and limitations on PPS effectiveness. Physical protection experts should provide their input in site identification during the Scope and Planning to prevent unnecessarily expensive or ineffective PPS implementation.

During this phase, physical protection experts should assist the entire pre-project team in determining the PPS grading, and work with the safety and safeguards experts to establish relative priorities among the 3S requirements. The task of 3S prioritization occurs throughout the facility lifecycle, and early development of a reconciliation process pays dividends later.

The Joint Japan-US team discussed reliability as a fourth element to the 3S requirements and rejected its addition. The reliability concept can be described as how reliability will be achieved in design and construction, and later sustained during operations and maintenance (the Operational phase). The notion of including reliability is derived from Architectural SuretySM. As used here, Architectural SuretySM is the construction of facilities that behave predictably in response to normal environments, abnormal environments, and malicious threats; for more details, see reference [45].

Initially, the Scope and Planning phase occurs outside of the project, but with the State's declaration to develop a NPP/NF, the Scope and Planning phase ends, and the NPP/NF enters the project phase. At this time, Scope and Planning becomes a project element as discussed in Section A.2, Project Phase.

A.2 Project Phase

Entry into the project phase follows the State's announced intent to build a NPP/NF. Associated with entry are the NEPIO inputs to the NPP/ NF project team forming the State's requirements and constraints for design, construction, and acceptance.

The Project phase is divided into five project elements, summarized as follows:

- 0: Scope and planning
- 1: Design Concept
- 2: Design Engineering
- 3: Construction
- 4: Acceptance

The project execution plan defines critical decisions (or CD's) and specifies actions to satisfy prior to exit from one project element and before entry into the next. A CD exists when the Design and Operating Agency, regulators (competent authority), and stakeholders must examine the project's performance relative to a set of performance-based expectations, and determine to commit funds for continuance, issue licenses for construction, or stop work if necessary. Typically, the project plan numbers the CD with respect to the concluding project element. For example, CD-0 Project Authorization occurs at the conclusion of the Scope and Planning project element and prior to Design Concept (Figure 4).

A.3 Leading to CD-0, Project Authorization

Scope and Planning (Project)

The PPT will use the physical protection objectives, site, environmental information, facility grading, and physical protection principles to conduct a high-level evaluation. The output of the evaluation is a PPS feasibility assessment, which the PPT provides to the project team⁶ for their consideration.

The project team will submit their results to the State's competent authority, and the Design and Operating Agency that will evaluate the 3S Site and Design Scope. If the 3S Site and Design Scope is satisfactory, the competent authority, and Design and Operating Agency will provide “project authorization.” Items in green are principal activities, and those items indented in orange text are essential outputs.

Figure 15 summarizes these actions leading to CD-0.

Scope and Planning			
Project Element	State	Design and Operating Agency	Physical Protection Team
Pre-project	Intent for new facility		
	Siting Criteria		
	Environmental Assessment		
	Laws, Regulations, Policy, and DBT(including URC)		
Scope		Site Selection	
		Method for selection	
		Site Document	
		Evaluation Document	
		Facility Grading	
		Scope Definition	
		Operational Concept	
		Physical Protection System Feasibility Study	
		DEPO: Feasibility	
Planning	3S Siting and Design Scope Review		
CD-0: Project Authorization			

Items in green are principal activities, and those items indented in orange text are essential outputs.

Figure 15. Scope and Planning

⁶ The project team, as envisioned in this first project element, is not fully formed. At CD-0 with project authorization, the project team will fully form, consistent with guidance found in the *Project Manager Body of Knowledge* [13]. Similarly, the PPT would comprise only staff sufficient to conduct the feasibility analysis.

A.4 Leading to CD-1, Conceptual Design

Concepts and Design Options

The first steps in the Conceptual Design (Figure 16) are the definition of the lifecycle requirements and the mission need statement.⁷ Using these inputs, the project team can develop the project definition, which describes the project organization, conceptual framework, milestones, and critical decisions. *The PPS concept, design, construction, and acceptance CDs must correspond to the project CDs. Failure to do so could result in increased implementation costs and, worse, a suboptimal PPS implementation when PPS requirements or modifications lag project progression.*

During the initial State discussions regarding the intent for nuclear power, the State should determine their implementing concept. Should the State opt for “turn-key” implementation with foreign sourced contractors and operators, an indigenous source for construction and operation, or a hybrid? Given the implementing concept, should the project team have both management and design responsibility? If only project management, then an Architectural and Engineering (A&E) firm should be engaged in conjunction with formation of the project team. The A&E team would then become the essential project group for design options, specification, and construction selection. The IAEA *Basic Infrastructure for a nuclear power project* [5] provides additional discussion on this topic.

Concurrent with Project Definition, the PPT examines PPS options and conducts a preliminary DEPO-like analysis of each. This PPT activity allows the PPT to evaluate potential designs with respect to meeting physical protection objectives. (Typically, these studies will form part of comprehensive 3S studies covering the options.)

The project team works in an iterative fashion to create and evaluate conceptual NPP/NF design options. During this phase, the project team and PPT should develop the initial Concept of Operations.

When the project team selects the preferred NPP/NF design option, the PPT should validate the chosen PPS option DEPO analysis and validate its currency. Once the validation is complete, along with other reviews such as safety and safeguards, the project team submits its design to the competent authority, and Design and Operating Agency for “conceptual design” acceptance and continuation into the Design Engineering phase.

⁷ The mission need statement as used in this document is the project team's assessment based on the gap between desired and existing capability (e.g., a need for nuclear power), the scope of the need, associated potential hazards arising from nuclear material, the associated 3S risk implications, and a rough order of magnitude assessment of NPP/NF project cost and schedule. The mission need statement is not an engineering study. Reference [46] provides an example.

Project Phase: Design Concept			
Project Element	State	Design and Operating Agency	Physical Protection Team
Project Definition	Safety Review		
		Lifecycle Requirements	
		Mission Need Statement	
		Project Definition	
		Design Options	PPS Design Options
Conceptual Design		Design Concept, Project Risk, and Budget Analysis	
			PPS Conceptual Design Selection
		Design Concept	
		Nuclear reactor establishment license application	
	Design Concept & Licensing Permit for NPP		DEPO: Options
CD-1: Conceptual Design			

Figure 16. Conceptual Design

A.5 Leading to CD-2, Design Approval

Design Engineering and Schematics

When the conceptual design has been accepted, the project team (including the A&E when used) creates the specific NPP/NF requirements leading to design definition. Concurrently, the PPT works to create a PPS design definition and further refine operational planning (Figure 17). The outputs of the PPT are as follows:

- PPS Design
- PPS personnel training and qualification plans
- Response force plans
- PPS Concept of Operations (ConOps)

Once finalized, the PPS design again undergoes a DEPO security analysis. The analysis assures that the PPS design remains consistent with vulnerability assessment and the current DBT. The PPT submits the PPS design requirements to the project lead and any 3S conflicts reconciled.

The PPT, working with the project team, should create the training and qualification plan, response force plans, and the ConOps. These are source documents for later site acceptance and continuous operations. As such, they should be maintained in the configuration management system.

The NPP/NF project and design definitions, including the PPS design, form the basis for project execution plan (PEP). Typically, the PEP will describe the design objectives, schedule, and cost.

Additionally, the PEP sets forth the roles and responsibilities for the project. As a communication tool, it must be continuously updated throughout all stages of the design process. The PEP sets forth critical steps for construction leading to site acceptance.⁸

The project team and A&E, when used, also develop sufficient design drawings to allow evaluation and later development of the contracting requirements. The project team presents the completed PEP with design drawings⁹ to the competent authority and the Design and Operating Agency for review and acceptance. With their “design approval,” the project moves into Construction phase.

Project Phase: Design Engineering			
Project Element	State	Design and Operating Agency	Physical Protection Team
Project Execution Plan			PPS Design
			ConOps
			Training and Qualification Plan
			Response Force Agreement
Manage Design	Design Review and Acceptance	Facility Design Definition	
		Project Execution Plan	
		Design review	
			DEPO: Design (final)
CD-2: Design Approval			

Figure 17. Design Engineering
(same as Figure 10 on page 41)

A.6 Leading to CD-3, Construction Approval

Contract Definition and Contract Award

The project team and A&E (if employed), using the approved design and related drawings, will author the contracting requirements (Figure 18). Concurrently, the PPT will develop the PPS design specifications leading to “PPS Contract Requirements.” Additionally, the PPT should develop and publish the “PPS Test and Acceptance Plan,” as well as a lifecycle plan for the PPS. The latter plan leads to publication of a “PPS Operations Logistics and Maintenance Plan.” The two plans are source documents, and the project team should maintain them in the configuration management system.

⁸ Project communications and control are essential. The PMBoK [13] is an excellent reference on the organization and processes to achieve these objectives.

⁹ "Drawings" has a broader meaning in this context and refers to both text and schematics to provide layouts, interfaces, specifications, and so on. The drawings are maintained in the project management information system, and should be under the configuration management system.

The PPS Test and Acceptance Plan might include specialized system and component tests. The PPS designs for a NPP/NF are tailored to the specific facility, which can result in specialized or unique subsystems and/or components. In these cases, the PPT may elect to build test beds to qualify subsystems and components prior to actual contractor procurement and facility installation. In these instances, the project plan should identify this pre-procurement process. The Test and Acceptance Plan should define acceptance criteria for these specialized systems and/or components, once they are installed.

The project team combines “PPS Contract Requirements” with the functional and remaining 3S contract requirements to produce a contract whose purpose is to allow suppliers to bid on the NPP/NF construction. The project team submits the contract to the competent authority, and Design and Operating Agency for their review and “construction approval.” Once the contract is approved, the Design and Operating Agency will tender the request for quote (RFQ) or similar process to potential suppliers.

Project Phase: Contracting			
Project Element	State	Design and Operating Agency	Physical Protection Team
Acquire Construction Supplier		Functional Design Specifications	PPS Design Specifications
			PPS Contract Requirements
			PPS Test and Acceptance Plan
			PPS Operations, Logistics, and Maintenance Plan
		Contracting Requirements	
		Contract Document	
		Application for construction permit	
	Construction Review and Approval		
CD-3: Construction Approval			

Figure 18. Contracting

A.7 Leading to CD-4, Acceptance

The project team and/or A&E firm (when used) will evaluate the RFQ responses and select the most suitable supplier. The PPT should evaluate the specific elements related to the PPS. Once the elements are selected, the Design and Operating Agency will award the contract and construction may begin (Figure 19).

Normally, a DEPO assessment would not occur during contract bid and award. However, the PPT should be part of the bid review and award process.

During the construction, the project team has responsibility to monitor progress and conduct construction quality reviews. The project quality-assurance system and project management information system (PMIS),¹⁰ as well as the configuration management system, should be fully implemented.

The quality assurance system¹¹ should establish intermediate inspection points during construction to verify the supplier meets design requirements. In this context, the PPT should also conduct PPS quality reviews. The “PPS Test and Acceptance Plan,” developed during contract definition is now used to measure successful installation of PPS subsystems and components. Part of the quality reviews is to update the DEPO analysis and validate that the design implementation still meets the physical protection objectives. The PPT team should also verify the DBT. If the DBT has changed, the PPT team should reevaluate the PPS design. Again, it is important to emphasize the difficulty of implementing later stage design changes. Due to extraordinary costs or infeasibility, it is possible the project team will reject late PPS design changes. Timely quality reviews can potentially reduce the likelihood of late changes.

Concurrent with the project team’s quality reviews, the competent authority will conduct periodic in-process construction inspections of critical structures and welds. Conceivably, these inspections might include performance inspections of the PPS as suggested by the JAEA Implementing Procedure flow (Figure 7).

¹⁰ The PMBoK [13] describes the PMIS as “an information system consisting of the tools and techniques used to gather, integrate, and disseminate the outputs of project management processes. It is used to support all aspects of the project from initiating to closing, and can include both manual and automated systems.” The PPT should use a PMIS to both transmit and retain records of PPS design information.

¹¹ The ASME NQA-1-2008 is common to the US nuclear industry and referenced in the US 10CFR 830.[20] NQA-1 states “Quality Assurance” comprises “all those planned and systematic actions necessary to provide adequate confidence that a structure, system, or component will perform satisfactorily in service.” Quality assurance includes quality control.

Project Phases: Construction			
Project Element	State	Design and Operating Agency	Physical Protection Team
Contracting		Contract Bid & Acceptance	
		Bid Evaluation	Evaluate PPS bid element
		Contract Award	
Construction		Start Construction	
			PPS Installation
		Construction Quality Reviews	PPS Testing and Performance Evaluations
			PPS Quality Reviews
			DEPO: Verification
	Critical structures and weld inspections		
		Prepare for Occupancy and Operations	

Figure 19. Construction

As construction completes, the project team will oversee preparation of the NPP/NF for occupancy and initial start-up operations. During this time, the PPT should conduct a quality acceptance of the full PPS. The team should verify the previously created "PPS Operations, Logistics, and Maintenance Plan," "PPS Test and Acceptance Plan," and "Response Force Agreement" source documents are in place and ready for NPP/NF start-up.

Upon completion of the project team quality acceptance, including the PPS acceptance, the competent authority will conduct a pre-service inspection. Based on the results from each, the competent authority and Design and Operating Agency will determine if the site is acceptable for unrestricted operations and "site acceptance."

Concurrent with site acceptance is project closing. During this last project action, all project management processes end, and the site management team assumes responsibility. During this period, plans should exist to transition the quality management and configuration management systems into sustained operations. As discussed in Section 4, SeBD Principles and Practices, the foundations for a robust, pervasive security culture should also be in place. The project team lead has responsibility to provide all necessary project information for sustained operations to the site management team, which includes the licensed engineer of the reactor for a NPP.

Figure 20 summarizes these key actions leading to "acceptance" of the facility.

Project Phases: Acceptance			
Project Element	State	Design and Operating Agency	Physical Protection Team
Acceptance		Conduct Quality Acceptance	
			Conduct PPS Acceptance
		Application for Safety, Physical Protection, and Safeguards plans approval	
	Pre Service Inspection		
	Safety, Physical Protection, and Safeguards Plan Approval		DEPO: Validation
CD-4: Acceptance			

Figure 20. Acceptance

A.8 Operational Phase

Prior to entering full, unrestricted operations, the NPP/NF should undergo an operational assessment. Typically, the operational assessment team will comprise independent experts and representatives of the competent authority. The team should, of course, include physical protection experts. Figure 21 summarizes the principal phase actions.

During the assessment, the physical protection experts will validate the PPS system performance, including the ConOp, Response Force Agreements, and Training and Qualification Program. All must be in place, fully implemented, and assure effective PPS operation. The earlier DEPO analyses should be reviewed, updated as necessary, and critical findings relayed to the site management team for resolution.

The competent authority will conduct a “Fitness to Operate” evaluation. The evaluation examines the human elements, technical elements, and operational concepts, including off-site support, such as the response force plan, to ensure they are fully integrated and functional. Based on a successful demonstration, the competent authority will permit the NPP/NF to enter full, unrestricted operations. The competent authority will notify the Design and Operating Agency, who will in turn notify the site management team, which includes the licensed engineer of the NPP reactor and the physical protection manager.

Once the NPP/NF is in the operational phase, the site management team will maintain suitable operation logs and records, sustain an effective quality and configuration management system, and promote a robust nuclear 3S culture. In addition to maintaining the operation logs and records, the Operating Agency (owner) should conduct security drills and investigate fully all security incidents.

The physical protection manager¹² should examine all records of drills and incidents, and periodically, the Operating Agency should initiate a PPS reassessment. These reassessments could be the result of a facility change, an incident, or a change in the State's DBT. A DEPO analysis should also be conducted on a periodic basis to validate that the PPS continues to meet its physical protection objectives. When findings indicate a significant deficiency, the Operating Agency should initiate remedial actions such as PPS subsystem upgrades or PPS replacement.

During the operational cycle, the Operating Agency and the State's competent authority will conduct planned and spot inspections to ensure safe, secure, and efficient operation, as well as continued conformance to the Comprehensive Safeguards Agreement (CSA). As the NPP/NF nears its planned or useful life, the State and Operating Agency may decide to “terminate operations” at the NPP/NF. Ideally, a decommissioning and dismantlement plan would exist prior to this decision. In this context, a DEPO assessment should be conducted to determine if any residual PPS requirements exist.

¹² The PPT should ensure that the physical protection manager receives all design drawings and significant information such as the Test and Acceptance Plan with results.

Operational Phase				
Project Element	State	Design and Operating Agency	Physical Protection Team	
Operational Test & Evaluation	Fitness to Operate	Operational Assessment		
		Qualified Staff		
		All systems start-up		
			PPS Operational	
			Response Force Agreements active	
			Training and Qualification Plan active	
			ConOp	
			Notify Physical Protection Manager	
			Notify Licensed Engineer of Reactor	
			Safety and Physical Protection Systems active	
Operational Cycle		Enter operational cycle		
		Operations and Maintenance Logs		
		Configuration management logs		
		Security drills and incident logs		
		Direct Surveys by Nuclear Safety Commission		
		Planned and Unannounced Inspections		
		Safety inspections		
		Physical protection inspections		
			Scheduled and Situational Facility Assessments	
			PPS Reassessment	
	DEPO: Reassessment (Planned)			
	DEPO: Reassessment (Situational)			
	Continue Operational Cycle			
Terminate Operations				

Figure 21. Operational Phase

A.9 Decommissioning and Dismantlement Phase

Once the decision has been made to terminate operation at an NPP/NF, a series of actions will take place to remove any remaining nuclear material inventory, environmentally restore some or all parts of the NPP/NF, and provide necessary safety, security, and safeguards for any remaining nuclear material or contaminated areas or structures, pending final dismantlement.

In some instances, portions of the facility containing nuclear material quantities of concern necessitating continued physical protection may not be immediately decommissioned. These residual PPS needs should be analyzed using a DEPO-like analysis, and appropriate PPS elements retained or modified. Figure 22 summarizes these actions.

Decommissioning and Dismantlement Phase			
Project Element	State	Design and Operating Agency	Physical Protection Team
		Application for Decommissioning Plan	Residual PPS Evaluation and Plan
	Approval of Decommissioning Plan		DEPO: Residual
	Approval of Revised Safety Plan		
		Application for Revised Safety Plan	
	Safety Inspection		
	Periodic Inspections		
		Application for Completion Check	
	Completion Check		
Decommissioned			

Figure 22. Decommissioning and Dismantlement

Appendix B - Evaluating Security Risk Assessment Factors

Figure 23 provides many PPS factors for use in a security risk analysis, which the PPT can use as one method during the Design and Evaluation Process (see Figure 4) to examine both vital and critical areas. The diagram could be used to populate a fault tree to determine unseen common mode failures and single point failures in the PPS design. Quantification may allow sensitivity analysis to examine the changes made during redesign.

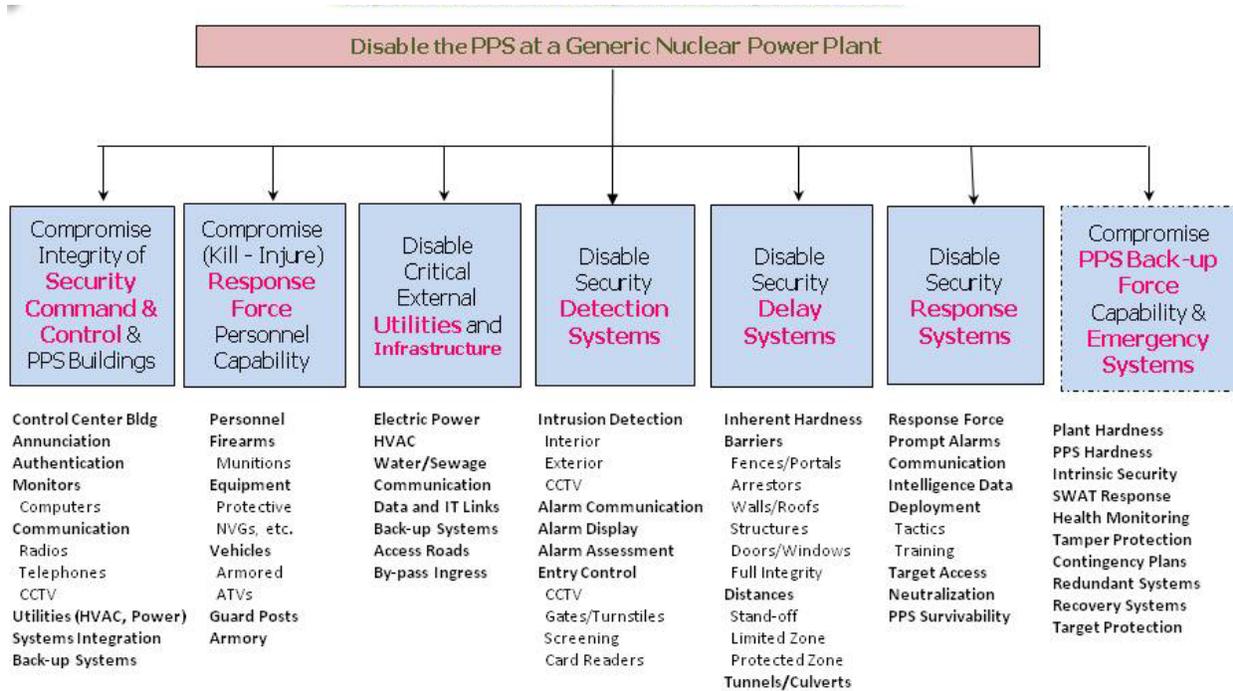


Figure 23. Security Risk Assessment Factors

Coincident with the development of risk factors leading to disablement of the PPS, the PPT should also evaluate the consequences. Typically, consequences measure impacts such as:

- Loss of human lives, safety controls, and health advantages
- Loss of economic and revenue benefits
- Loss of national security and government functionality
- Psychological stress caused by destruction of iconic and symbolic assets
- Loss of public confidence in national stability
- Loss of sensitive information

As one can readily ascertain, these consequences can be common to all 3S disciplines. Hence, as the consequences are assessed by each 3S discipline, cross comparisons can be made to facilitate developing a method to reconcile potentially conflicting 3S requirements. Quantification of

consequences can be difficult and subject to the State's definition. However, when quantification is used or allowed, the PPT should construct "consequence bins" to characterize the outcomes.

One approach to constructing "consequence bins" is to create a list of undesired events for an NPP, such as loss of reactor and containment building, loss of turbine-generation systems, loss of water supply and cooling systems, and so on. Then the undesired event can be matched with its consequence measure, (such as radioactive material release) and consequence values can be assigned (for example, curies of released material). The quantified values can then be binned, using qualitative terms such as "high," "medium," or "low." Similarly, the consequence table might include areas critical to the PPS functionality as suggested in Figure 23. Combining the consequence bin with assessed likelihood enables creation of a risk matrix that allows 3S comparison.

Appendix C - Security Risk Management

The risks analysis approach described in the previous section provides a consistent and auditable method that can be extended to cover 3S risk management. While security is the focus of this document, the overarching objective of a PPS design is to allow the mission and ensure security exceeds the potential threat. In the 3S context, the mission includes meeting safety and safeguard requirements. Budgets, functional requirements, and the other 3S requirements are constraints in the PPS design. Hence, the project team must create a prioritization matrix to reconcile potentially competing functional and 3S requirements, and allocate constrained resources. One method follows:

1. Compare all vital and critical areas and assign a rank ordering of each (horizontal comparison). For example, the project team could elect to use the IAEA radioactive release threat levels to achieve the rank ordering.
2. Compare the 3S elements within each vital or critical area (vertical comparison)
 - a. Subject matter experts from each 3S discipline should use pair-wise comparisons to establish relative priority.
 - b. The comparisons must be rank ordered.
3. Risk management alternatives should be explored when unacceptable compromises exist in any of the 3S disciplines.
4. Resources should be applied consistent with the prioritization matrix.

When examining the risk management alternatives, the PPT may use the following logic diagram to evaluate potential alternatives (Figure 24). The process of risk management is recursive, and as alternatives are identified, the project team should evaluate them again for potential conflicts with other 3S elements and take appropriate actions for reconciliation.

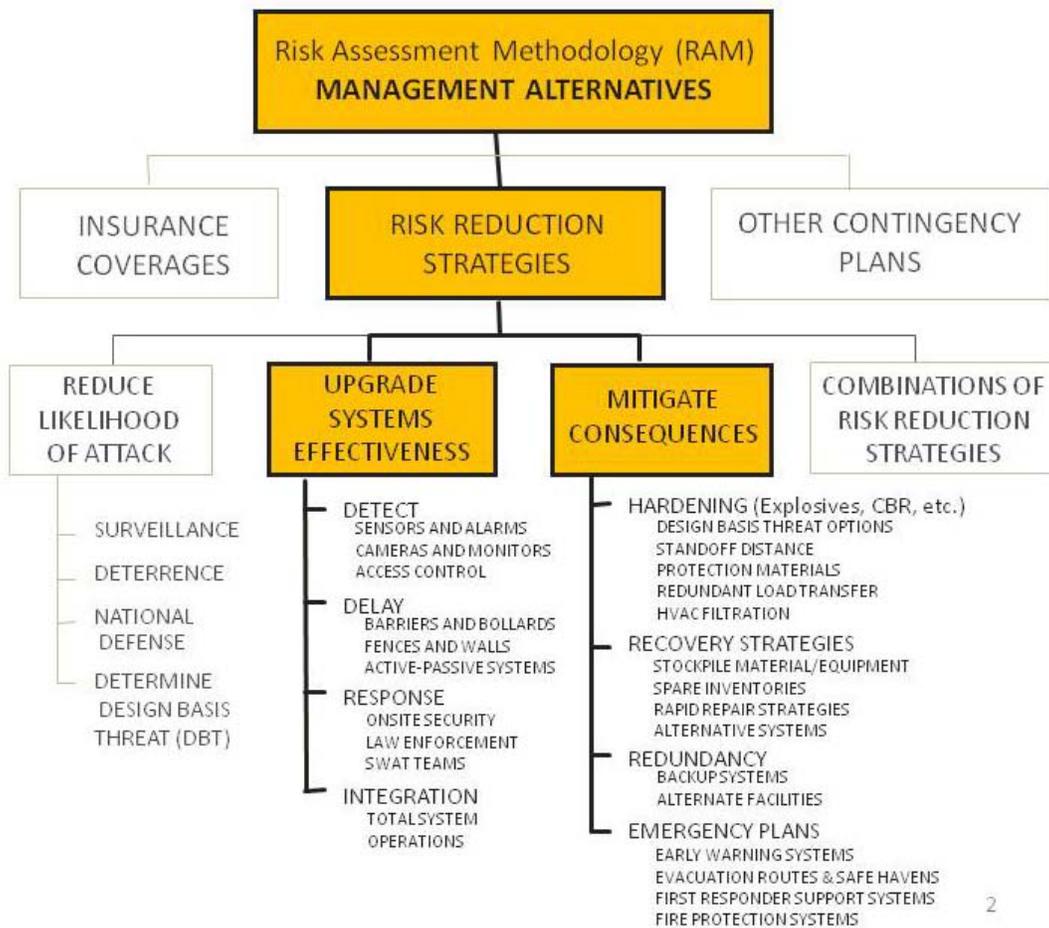


Figure 24. Risk Assessment Management Alternatives

Appendix D – Relationship of Lifecycle Phases and Certain Project and Security Activities

The following diagrams (Figure 25 - Figure 28) show how many of the activities during the lifecycle phases are connected, whether in terms of precedence, decision points, or data flows.

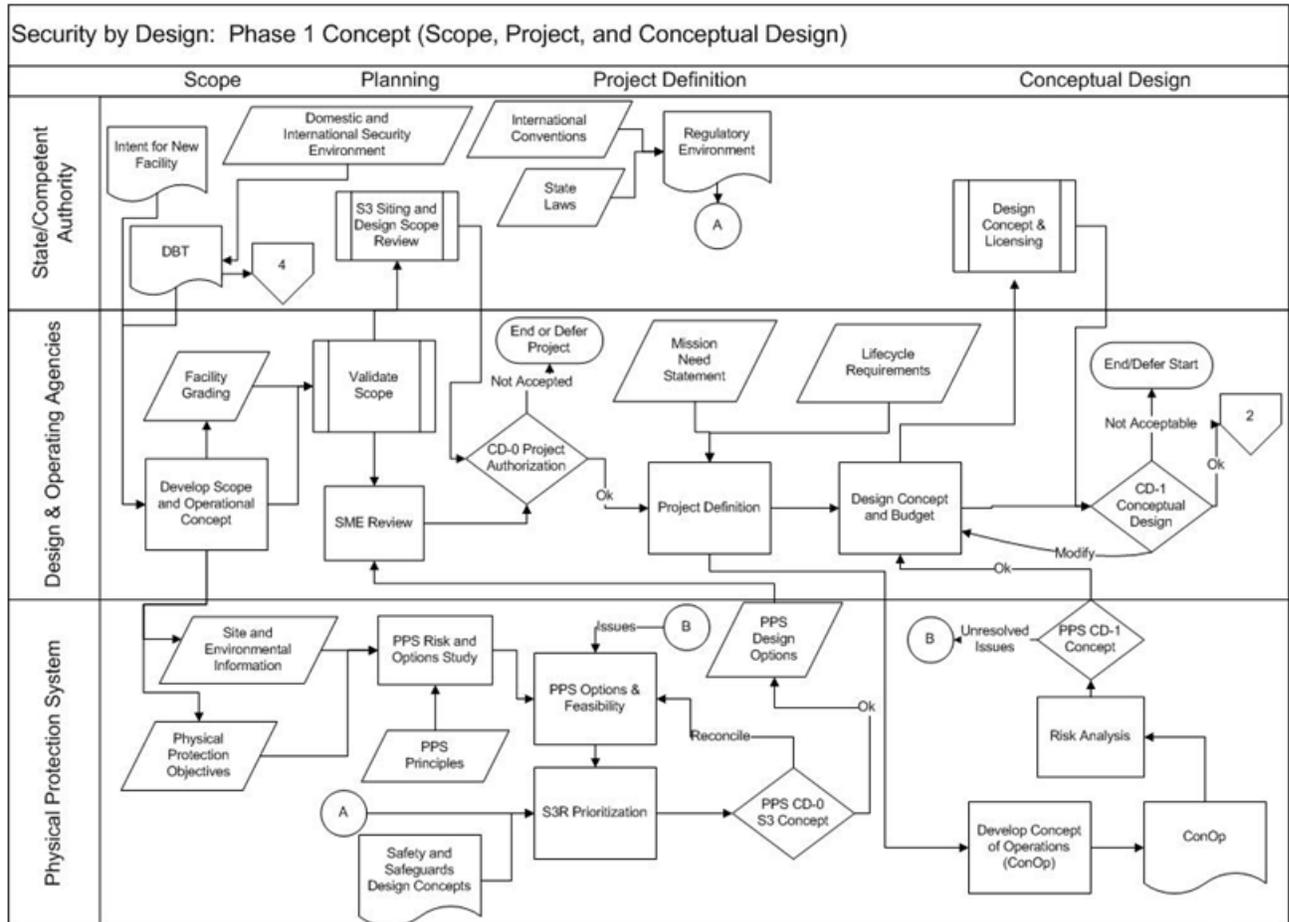


Figure 25. Activities during Scope, Planning, Project Definition, and Conceptual Design

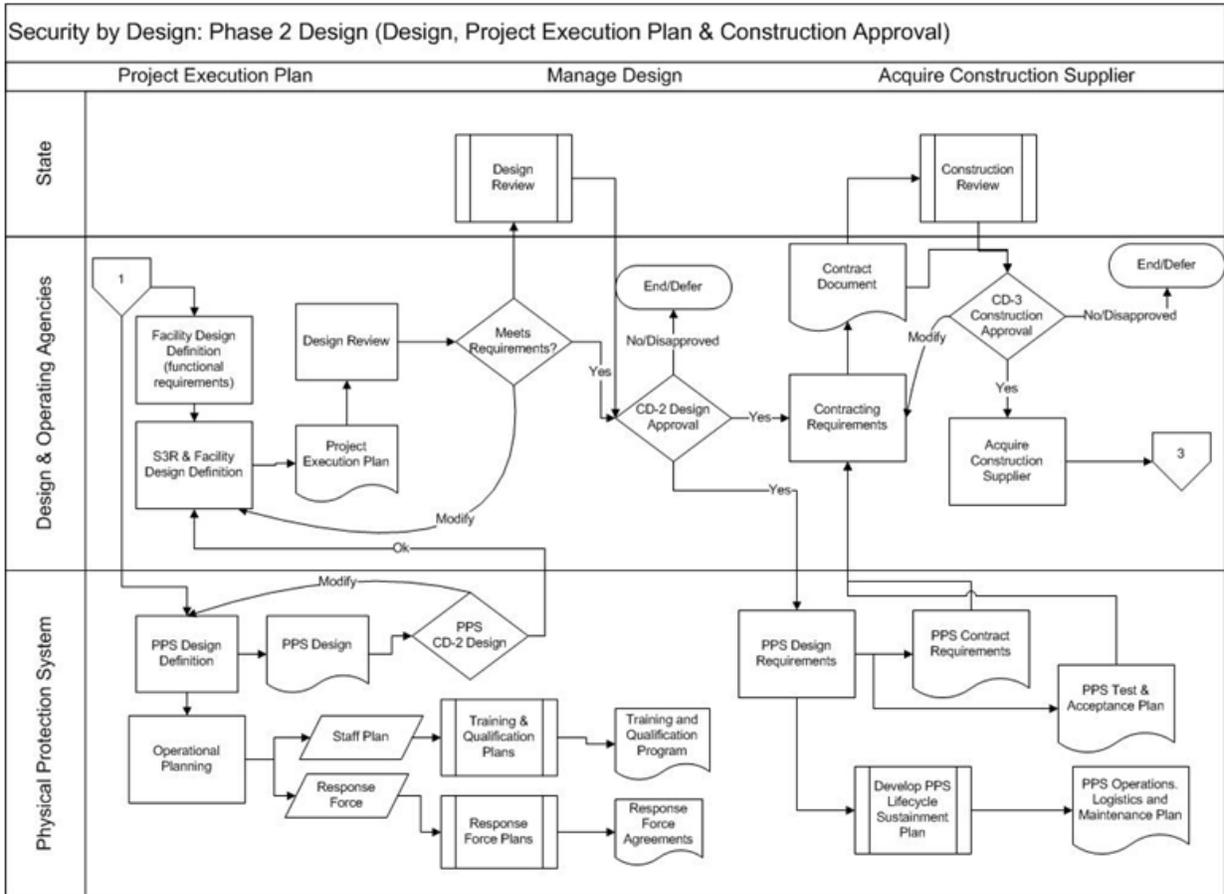


Figure 26. Activities during Design Engineering and Contracting

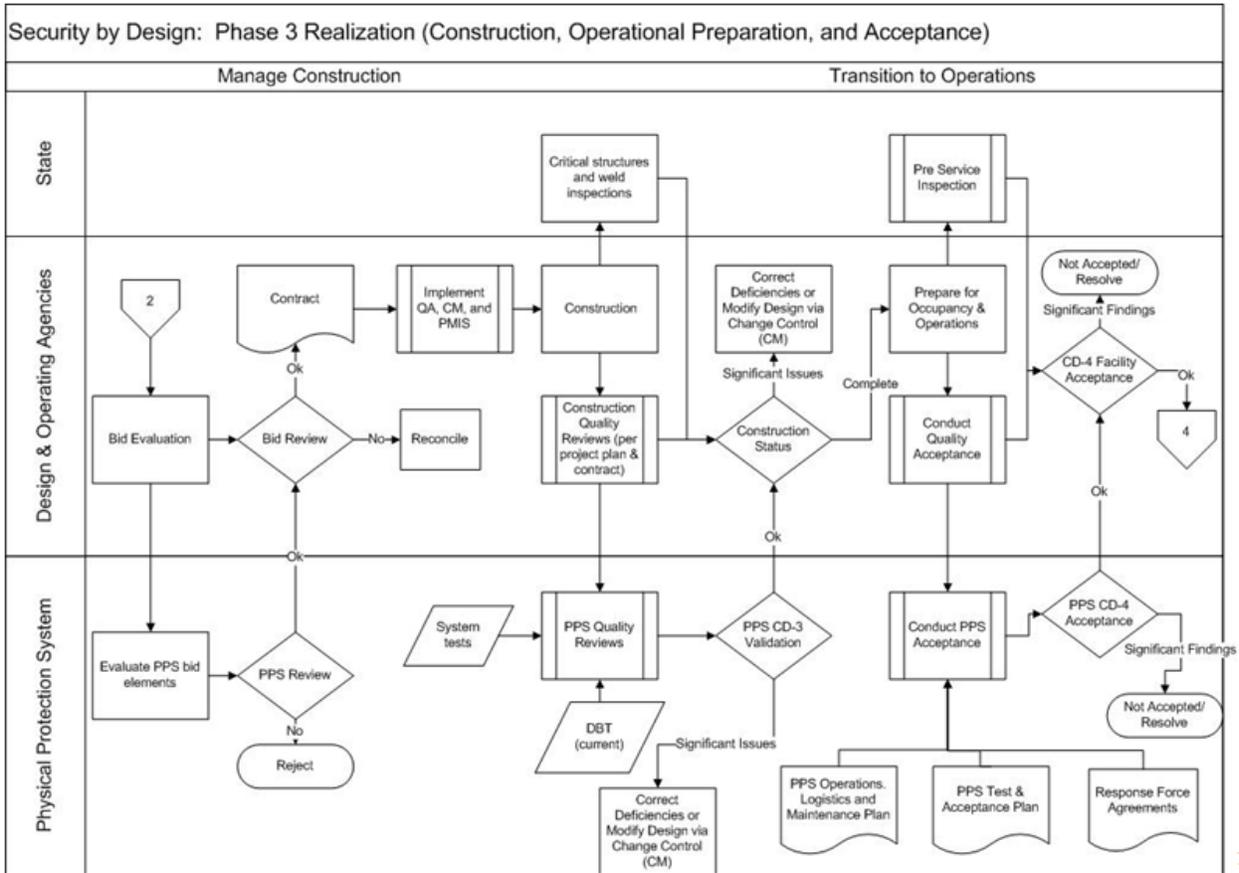


Figure 27. Activities during Construction and Fitness to Operate (Transition to Operations)

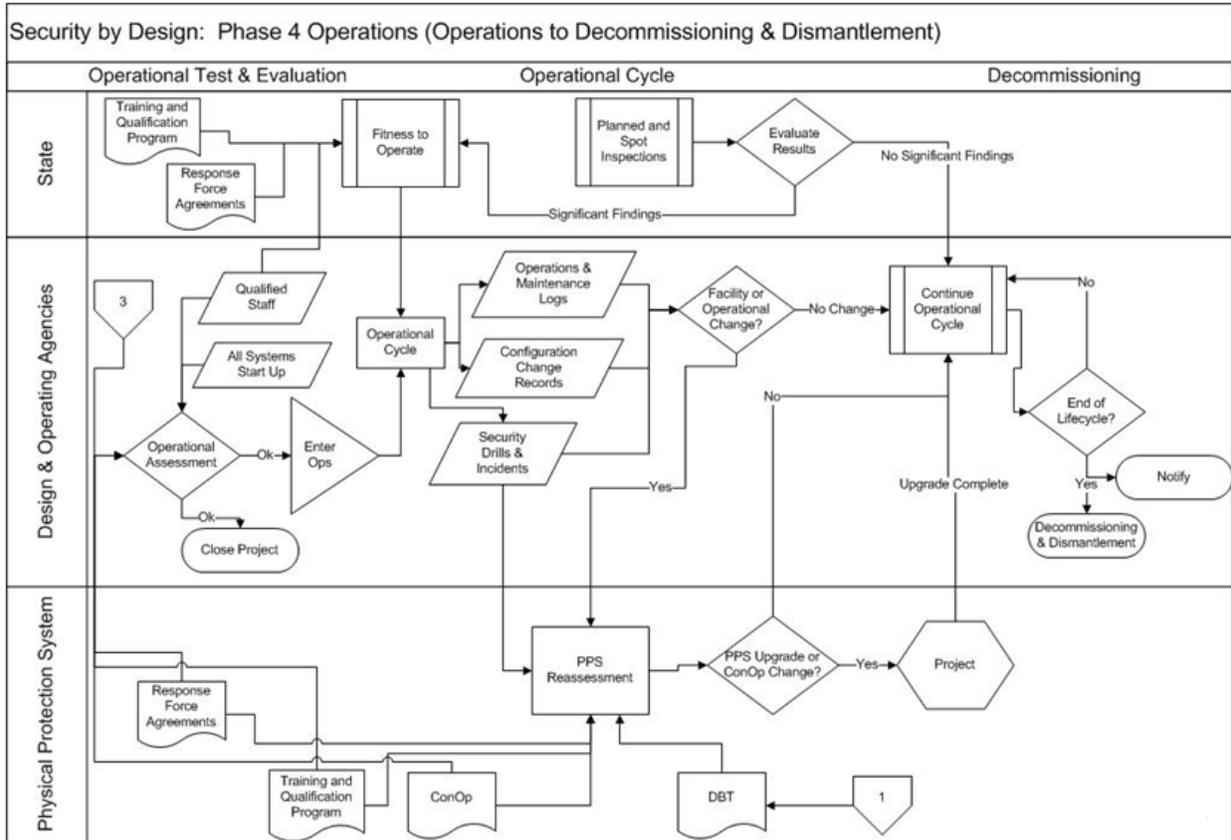


Figure 28. Activities during Operations and Decommissioning/Dismantlement

Appendix E – More Information on the Principles and Practices

E.1 Introduction

Section 4, the SeBD Principles and Practices section, has a short section on each principle, along with a discussion of the associated practices. The discussion for each principle is limited to about 2 pages.

This section includes more information concerning some of the principles and practices that was considered too detailed or extensive to fit in section 4. This information on the Fundamental Principles A-L and the Other SeBD Principles is grouped into six topical areas:

- Topical Area: Management Principles - include topics such as organizational responsibility, whether the State, competent authority, or licensee; the need for a legislative and regulatory framework; and use of balanced requirements and grading.
- Topical Area: Physical Protection Principles - The PPS needs to be based on the threat, reflect graded protection, and provide defense in depth. Ideally, physical security should exploit facility features that can intrinsically enhance security.
- Topical Area: General Technical Principles - The PPT will use proven project management techniques and good engineering practices.
- Topical Area: General Human Element Principles - These principles include proven human resource and security practices.
- Topical Area: Systems Engineering Principles - Nuclear facilities (in general) and Physical Protection Systems (in particular) are designed and built using good systems engineering principles.
- Topical Area: Other Specific Principles - Other specific principles include quality assurance (Fundamental Principle J), configuration management (Fundamental Principle J), contingency plans (Fundamental Principle K), effective communications (Other SeBD Principle—Validate Effective Communication and/or Operational Agreements with Other Agencies), and exchange of experience (Other SeBD Principle—Project and Operations Experience).

Table 5 below shows how the Fundamental and Other SeBD Principles are assigned to the different Topical Areas.

Topical Areas that have further information on principles and practices are covered below.

Table 5. Topical Groupings of the Fundamental Principles and Other SeBD Principles

Management Principles	Physical Protection Principles	General Technical Principles	General Human Element Principles	System Engineering Principles	Other Specific SeBD Principles
Fundamental Principle A—Responsibility of the State	Fundamental Principle G—Threat	Fundamental Principle E—Responsibility of the License Holders	Principle—Proven Operational Planning	Principle—Use good systems engineering principles	Fundamental Principle J—Quality Assurance
Fundamental Principle B—Responsibilities during International Transport	Fundamental Principle H—Graded Approach	Fundamental Principle J—Quality Assurance		Principle—View the PPS from a lifecycle perspective	Fundamental Principle K—Contingency Plans
Fundamental Principle C—Legislative and Regulatory Framework	Fundamental Principle I—Defense in Depth			Principle—Use a Concept of Operation perspective	Principle—Validate effective communication and/or operational agreements with other agencies.
Fundamental Principle D—Competent Authority	Principle—Achieve Inherent Security				Fundamental Principle L—Confidentiality
Fundamental Principle E—Responsibility of the License Holders				Principle—Synergy between Safety, Safeguards, and Security	Principle—Project and Operation Experience
Fundamental Principle F—Security Culture				Principle—Adopt design-in sustainability	
				Principle—Balance prescriptive and performance-based requirements	

E.2 Topical Area: Management Principles

One Fundamental principle that falls under this topical area is Security Culture, covered by an implementing guide, reference [15], which describes some key factors associated with security culture that are heavily influenced by management especially, and by other personnel:

- a) Beliefs and Attitudes: “The beliefs and attitudes held by individuals are influenced by the actions that others take or do not take and also by what others (particularly top managers) say or do not say. In this way, beliefs and attitudes spread and replicate themselves within organizations.” “Without a strong basis of beliefs and attitudes [that a credible threat exists and that nuclear security is important], an effective nuclear security culture will not exist.”
- b) Motivation: Motivation, the key determinant of behavior, is entirely dependent upon the internalization of beliefs and values. However, the performance of individuals is significantly influenced by the encouragement and reinforcement received from leaders, peers, and subordinates.
- c) Leadership: The greatest influences on individual performance are the expectations of leaders. Nuclear security is most effective when managers and supervisors of the organization continually demonstrate their commitment to security through their words and actions.

This Implementing Guide describes a set of security culture indicators that are useful for assessing nuclear security culture; these indicators can be evaluated early in the design process (e.g., during scope and planning or during the design concept phase) to evaluate strengths and weaknesses of the security culture that need to be addressed in the design. Three examples of such factors include:

- Given the State’s level of security culture, are there certain behaviors that are considered acceptable even though they have a negative impact on security? Examples include employees taking security cabling for resale, propping doors open during smoke breaks, and leaders/managers not observing fully access control or contraband policies.
- Social factors that might hinder proper implementation of security culture, such as polarization between management and workers, tribal/ethnic differences, use of foreign workers, and religious differences.
- Status differences where lower-status employees are either reluctant or prevented from challenging higher-status employees.

Considering these factors during both requirements definition and design can help minimize the negative effect of these factors on the actual facility.

E.3 Topical Area: Physical Protection Principles

The PPT will use the physical protection objectives, site, environmental information, facility grading, and physical protection principles to evaluate the design. The protection theme is based on the threat

assessment, uses a graded approach, ensures defense in depth and, as much as possible, employs features that can enhance security intrinsically. Some references on the topic of physical protection are [47], [48], and [35].

In the early facility-planning phase, siting and general facility characteristics can be important aspects affecting the physical protection design. Many factors need to be taken into account including geography, climate, nearby population, cultural acceptance of security approaches, local availability of skills and expertise, weaponry, authorizations for the use of deadly force, etc.

Best Practices for Physical Protection

The Institute of Nuclear Materials Management developed a list of Global Best Practices for Physical Protection, at a Special International Workshop on Global Best Practices in Physical Protection, held June 14-18, 2004; see reference [49]:

A PPS is a complex configuration of detection, delay, and response elements. Techniques must be applied to evaluate the physical protection system against the defined threat (DBT). For most analysis models, the targets and the series of actions against targets must first be identified for both theft and sabotage. These actions must be either modeled, simulated, or exercised to determine the performance of the physical protection system of the facility. If computer models are used to determine performance, it is very important that the data used to represent detection, delay and response for the facility is as accurate as possible...

- Regularly scheduled performance tests on each element of the physical protection system are useful in determining the current effectiveness and potential degradation of hardware. Multiple and replicated data points (statistically supportable) should be used in the analysis of detection, delay, and response.
- Every change to the PPS must be reevaluated. Whenever the physical protection system is upgraded or components are replaced, performance tests must be conducted to validate that the component is providing the required capability.
- Assessment tools must be used in concert with each other, such as computer analyses using the results of performance tests and expert opinion. Employing more than one performance assessment tool or technique can be helpful in validating PPS effectiveness.
- If the threat evaluation changes (for either the outsider or the insider) during the facility lifecycle, then the PPS effectiveness should be reevaluated.
- Always focus on the performance intent of a requirement.

Design Basis Threat and Threat Assessment

The DBT or threat assessment (TA) is developed and used to provide assurance that adequate protection is provided. Changes in the threats may result in a need for modifications of the DBT/TA to continue to provide adequate assurance of effective protection.

The DBT/TA works as a design/evaluation standard by setting boundaries on the attacker capabilities and scenarios they can perform. Adequate physical protection is then provided by designing a PPS that is effective against the entire DBT/TA.

A number of important topics are associated with this practice:

How does one set up the process for defining a DBT/TA?

This is described in IAEA Nuclear Security Series No. 10, “Development, Use and Maintenance of the Design Basis Threat,” an Implementing Guide [16]. There is an associated IAEA workshop on Setting the Design Basis Threat that can be used by a State to start development of a threat assessment or Design Basis Threat. This workshop is quite useful in bringing the right specialists together (often for the first time) to consider threat issues.

What is the distinction between the Threat Assessment and the Design Basis Threat?

Both start by looking at information about threats of or actual attacks on nuclear facilities by terrorists and other groups that are committed locally, nationally, and internationally. Sophisticated attacks against other targets, such as banks, can also be examined. Both capabilities and motivations of the attackers are considered. Note that data should be collected on both insider threats (with access to the facility) and outsider threats (with no access to the facility). The threat assessment analyzes this information to infer particular threat entities (such as specific terrorist or criminal groups), their motivations and intentions for an attack, and their capabilities (such as weapons and numbers); see Table 6 below:

Table 6. Outsider Threat Matrix

Outsider Threat			
	Threat Entity 1	Threat Entity 2	Threat Entity 3
Motivations			
Intentions			
Capabilities			
Size of Group			
Weapons			
Explosives			
Transportation			
Power and Hand tools			
Technical Skills			
Level of Funding			
Infrastructure			

The insider threat can be described in terms of characteristics of the categories of personnel that have access to the facility:

- Access to areas of a facility, systems, equipment, or tools
- Authority over operations or personnel
- Knowledge of facility layout, transport arrangements and/or processes, physical protection, safety systems and other sensitive information
- Technical skills or experience
- Authority to acquire and ability to use tools, equipment, weapons, or explosives [50]

The DBT differs from the threat assessment in that it 1) screens out those threats that lack the motivation, intention, or capability to commit a malicious act involving nuclear materials and nuclear facilities; 2) Combines the information about the threat entities into a composite adversary with postulated capabilities; and 3) modifies the postulated capabilities of the composite adversary based on relevant policy considerations.

What is the value of a DBT over a TA?

If done properly, a DBT is a policy document that provides a stable basis for security planning over long time horizons, allows efficient use of whatever security resources are available, and provides a rationale for why additional resources are not being required. A TA can perform some of these functions to a limited extent. Put another way, without a properly scoped DBT (updated periodically) licensees will overspend and under-protect their nuclear assets.

However, to take advantage of the DBT/TA properly, the State should possess the expertise to properly evaluate the effectiveness of the PPS against the DBT/TA. To perform this evaluation, the DBT/TA may be used as a basis to:

- Develop potential adversary scenarios, and
- Conduct an analysis of the effectiveness of the protection system.

How is the DBT/TA used?

There are actually a number of options:

1. The Competent authority provides the DBT/TA to the operator along with guidance on effectiveness of PPS to protect against it.
2. The Regulator establishes performance requirements based on the DBT and provides performance requirements to the operator.
3. The Regulator defines prescriptive requirements based on the DBT and provides these to the operator.

In deciding which approach is the most appropriate, a State needs to consider several State-specific factors:

- The competence of the operator to interpret performance requirements
- The number of facilities in a State and the impact of limiting flexibility of a facility to develop the optimum solution
- The severity of the potential consequences

In today's environment, what are some key factors in developing a TA/DBT?

Historically, TAs and DBTs have focused on attacks by outsider threats (such as terrorist groups). In today's environment, it is suggested that States focus more effort than in the past on designs countering cyber-attacks, insider attacks, standoff attacks, and aircraft impacts. Where such threats cannot be stopped with traditional physical protection, designs should consider the integrated effectiveness of physical protection, material accountancy and control (at the domestic level), operational/process controls, and emergency response.

Interplay of Facility, Threat, and Targets

The three topics for defining PPS requirements—characterize facility, define threat, and identify targets—are not entirely independent. Each must be considered while taking into account knowledge of the others. For example, the types of adversaries are probably dependent on the types of facility targets.

It is important to characterize facility risks of theft of nuclear material and radiological sabotage and develop designs with increasing protection levels for facilities with greater consequences.

Implementing a Graded Approach

A first-order task is to characterize facility risks of theft of nuclear material and radiological sabotage, and develop designs with increasing protection levels for facilities with greater consequences. Actions and associated references include identifying a target categorization scheme (for example, IAEA Category I nuclear material at facility) to guide facility design. See References [3], [36], [51], [29], and [52].

Identifying and Protecting Targets

Questions to Identify Targets

Target identification is a multi-faceted problem that can be approached as a series of questions.

1. What do we have that needs protection? (What are potential targets?)
2. Are there different operational conditions that must be considered?
3. What is the target worth to us?
4. How attractive is the target to those who are interested in its theft, damage, or destruction?
5. Where, specifically, is the target located?

At most nuclear facilities, nuclear materials appear in several different physical and chemical forms. The attractiveness of these materials as theft or sabotage targets depends greatly on their form, since the form of the material determines its ease of acquisition by the potential thief, as well as the ease of subsequent malicious use. In light water reactors, for example, nuclear material appears in four forms: fuel assemblies, solid wastes, liquid wastes, and gaseous wastes. These materials rank differently in terms of their attractiveness to a potential saboteur or thief.

Four-Step Process to Identify Targets

Target identification has been presented as a foundational requirement to security system design. For facilities concerned with theft or sabotage of nuclear and radiological materials, target identification, as a process, can be described by the following steps:

1. Develop an understanding of the applicable security policies with attendant goals or objectives.
2. Identify the types of nuclear and radiological materials and nuclear systems (e.g., reactors or material process lines) that must be protected from theft and sabotage at the particular facility of concern.
3. Identify the appropriate categorization (consequence) levels that apply for each theft and sabotage target located at the particular facility of concern.
4. Develop a target list for the facility to include target description, category, and location (area) to be protected. This may require use of itemization, walk downs, and other advanced target identification techniques.

Target Types—What Should Be Protected?

1. Protect nuclear material from theft that could lead to the construction of a nuclear explosive device by a technically competent group.¹³
2. Protect radiological material from theft that could lead to the construction of a radiological dispersal device.¹⁴
3. Protect nuclear and radiological material in use or storage from sabotage that could directly endanger the health and safety of personnel, the public, and the environment by exposure to radiation or release of radioactive substances.¹⁵

The difference between target type 3 and type 2 above is that the threat uses conventional explosives or mechanical means to disperse radiological materials in situ (or at least at the facility where the materials are located) rather than in some other location of their choosing.

4. Protect nuclear facilities (systems) from sabotage that could indirectly endanger the health and safety of personnel, the public, and the environment by exposure to radiation or release of radioactive substances.

The difference between target types 4 and type 3 is that the threat uses the inherent energy available in nuclear materials (decay heat for irradiated or spent fuel and nuclear energy in reactor core assemblies or subassemblies) to disperse radiological materials in situ.

Target Categorization for Unauthorized Removal

The INFCIRC/225/Revision 5, reference [3], Nuclear Material Categories, Table 7 in this handbook, is an example of a target categorization scheme. The application of such a scheme along with associated references, such as References [3], [36], [51], [29], and [52], can be used to guide facility design.

Categorization Basis

IAEA categorization of nuclear materials is based on four attributes: element, isotopic concentration (e.g., uranium enrichment), mass, and irradiation history (or radiation level). The primary categories of concern are labeled I, II, and III, with Category I representing the highest-risk material. The categorization table from INFCIRC/225/Revision 5 [3] is presented in Table 7 below.

¹³ Compare INFCIRC/225 Revision 5 [3], §4.1-4.4.

¹⁴ This could include use of the material passively (e.g., unshielded source placed in a public area) or in an active design (dispersed using conventional explosives or by mechanical means).

¹⁵ Compare INFCIRC/225 Revision 5 [3], §2.1.

Table 7. INFCIRC/225/Rev 5 Table 1 Covering Nuclear Material Categories

Material	Form	Category I	Category II	Category III^c
1. Plutonium ^a	Unirradiated ^b	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235	Unirradiated ^b – uranium enriched to 20% ²³⁵ U or more – uranium enriched to 10% ²³⁵ U but less than 20% ²³⁵ U – uranium enriched above natural, but less than 10% ²³⁵ U	5 kg or more	Less than 5 kg but more than 1 kg 10 kg or more	1 kg or less but more than 15 g Less than 10 kg but more than 1 kg 10 kg or more
3. Uranium-233	Unirradiated ^b	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated Fuel (The categorization of irradiated fuel in the table is based on international <i>transport</i> considerations. The State may assign a different category for domestic use, storage, and <i>transport</i> , taking all relevant factors into account.)			Depleted or natural uranium, thorium, or low-enriched fuel (less than 10% fissile content) ^{d,e}	
<ul style="list-style-type: none"> • ^a All plutonium except that with isotopic concentration exceeding 80% in plutonium-238. • ^b Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/hr (100 rad/hr) at one meter unshielded. • ^c Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice. • ^d Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection. • ^e Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/hr (100 rad/hr) at one meter unshielded. 				

In a nuclear reactor, the greatest concern in the design of a PPS is to prevent radioactive release from the reactor that may be caused by sabotage. Vital areas (those areas within a reactor complex that contain equipment, systems, devices, or material whose failure, destruction, or misuse could result in a radiological release endangering the public) are of particular concern. For example, the containment building that houses the reactor, the steam generators, and the primary coolant loops will always be designated a vital area. Other locations containing machinery and safety systems designed to decrease the severity of accidental damage to nuclear facilities may also require designation as vital areas.

Vital Area Protection and Vital Equipment

Reference [53] describes USNRC guidelines on what equipment to protect as vital. Under these guidelines, vital equipment includes the following:

One train of equipment (with the associated piping, water sources, power supplies, controls, and instrumentation) that provides the capability to perform the functions (reactivity control, decay heat removal, and process monitoring) that are necessary to achieve and maintain hot shut down for a minimum of eight hours from the time of reactor trip, plus the major components of the reactor coolant makeup system and associated support equipment necessary to achieve this goal.

Equipment examples include, but are not limited to the following:

Reactivity control—control rod scram components and systems.

Decay heat removal—turbine-driven auxiliary feedwater pump, including control, water source (e.g., condensate storage tank), and main steam safety valves (for pressurized water reactors (PWRs)). Turbine-driven, high-pressure core injection (HPCI), reactor core isolation cooling (RCIC) pump, isolation condenser, including auto start, control, and safety-relief valves (for boiling water reactors (BWRs)).

Process monitoring—pressurizer pressure and level, steam generator pressure and level, reactor coolant hot and cold leg temperature (for PWRs); reactor pressure and level, suppression pool temperature and level (for BWRs).

Reactor coolant makeup and reactor coolant pump seal cooling—charging pump, including water source and motor control center (for PWRs).

Support functions—diesel generator, including switchgear, cooling, startup, and controls (for PWRs and BWRs). Battery (for PWRs and BWRs). Service water pump and motor control center (for PWRs and BWRs). Component cooling water pump and motor control center (for PWRs).

- The reactor vessel and reactor coolant piping up to and including a single, protected, normally closed isolation valve or protected valve capable of closure in interfacing systems. Note this precludes the need to protect Loss of Coolant Accident (LOCA)-mitigating equipment.
- The control room and any remote locations from which vital equipment can be controlled or disabled (such as remote shutdown panels, motor control centers, circuit breakers, or local control stations).

- Cable terminals or junctions and areas such as cable spreading rooms. Cable runs in trays and conduit need not be protected unless cables necessary for safe shutdown capability are individually identifiable and the identification is reasonably accessible.

Note that when any components or systems protected as vital are inoperable (e.g., during maintenance), appropriate compensatory measures (such as stationing guards at alternate locations) must be taken to ensure the ability to reach hot shutdown.

Sabotage

Definition—The IAEA defines sabotage¹⁶ as: “Any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive substances.”

Unlike the cases discussed for the protection of nuclear and radiological material from theft, where varying theft consequences were managed through the surrogate of categorization, the current approach to identifying sabotage as a potential target begins with a yes or no proposition; either you have to protect against it or you don't. At that point the “level of the physical protection measures should be specifically designed to take into account the nuclear facility or nuclear material, the State's design basis threat and the radiological consequences.” That is, the problem is twofold. First it must be determined if the DBT is capable of an act of sabotage that would lead to unacceptable radiological consequences (presumably in the form of some threshold measures related to the endangerment of personnel, the public, and the environment). If so, the next task is to use some means to develop a PPS design and evaluate its performance versus the DBT in order to demonstrate that risk has been mitigated to an acceptable level.

Unacceptable Radiological Consequences

States have many options on how to define unacceptable radiological consequences. One possible approach would be to look to the safety realm for guidance. For instance, consider the safety-related radiological acceptance criteria discussed by IAEA NS-R-1 [54] paragraph 5.69:

“...the design basis for items important to safety shall be established and confirmed. It shall also be demonstrated that the plant as designed is capable of meeting any prescribed limits for radioactive releases and acceptable limits for potential radiation doses... “

That is to say, sabotage criteria might be based on some design basis (e.g., no core damage), potential radioactive release, or radiation dose levels (or some combination thereof), but this is not to say that radiological sabotage criteria should be the same—quantitatively—as safety criteria; establishment of any such criteria is a decision for appropriate national authority. However, to illustrate such criteria,

¹⁶ INFCIRC/225/Revision 5 [3], Under Definitions on page 53.

consider the following US 10 CFR 100 [55] requirements (NS-R-1 does not provide quantitative recommendations):

“... an individual located at any point on its [facility] boundary for two hours immediately following onset of the postulated fission product release would not receive a total radiation dose to the whole body in excess of 25 rem or a total radiation dose in excess of 300 rem to the thyroid from iodine exposure. (10 CFR 100.11(a)(1)).”

Safety Assessment

Given some form of a safety assessment that provides a quantitative measure of the potential impact at the site boundary (as in 10 CFR 100 above [55]) or other suitable control point (e.g., nearest population center), it is easy to imagine, a radiological sabotage categorization scheme by analogy with the theft categorization examples. For example, if the two-hour dose at the boundary were less than 25 rem, this could be defined to be a Category 4 facility. Then, assuming a power of ten is appropriate (but recognizing the exposure mechanisms of concern and the actual criteria for establishing different category levels is a policy issue), a two-hour dose of 25-250 rem would be assigned to Category 3, 250-2500 rem to Category 2, and 2500 rem or more to Category 1. A similar scheme for worker and environmental impacts could be developed.

Once the categorization method is determined, the possibility of theft and sabotage against the facility or material and the acceptable risk level should be considered.

Risk Scales

In contrast to taking a quantitative approach, expert judgment could be used to develop relative risk scales. For example, a scale was developed and published for use in assessing sabotage risks of various spent fuel disposal alternatives; see reference [56]. Such relative risk scales could provide a means of system sabotage categorization for use in physical security system design.

Use of the International Nuclear Event Scale

Another approach to consider would be possible use or adaptation of the International Nuclear Event Scale published by the IAEA and shown in Table 8. This could be accomplished by mapping the estimated consequences of a particular postulated sabotage action to the criteria presented in the table (note that multiple attributes are expressed in the criteria column).

Table 8. International Nuclear Event Scale

Level/ Descriptor	Off-Site Impact	On-Site Impact	Criteria	Examples
ACCIDENTS 7 Major Accident	<i>Major Release:</i> Widespread health and environmental effects		External release of a large fraction of the radioactive material in a large facility (e.g., the core of a power reactor). This would typically involve a mixture of short- and long-lived radioactive fission products (in quantities radiologically equivalent to more than tens of thousands terabecquerels of iodine-131). Such a release would result in the possibility of acute health effects; delayed health effects over a wide area, possibly involving more than one country; long-term environmental consequences.	Chernobyl Ukraine, 1986
6 Serious Accident	<i>Significant Release:</i> Likely requires full implementation of planned countermeasures		External release of fission products (in quantities radiologically equivalent to the order of thousands to tens of thousands of terabecquerels of iodine-131). Such a release would be likely to result in full implementation of countermeasures covered by local emergency plans to limit serious health effects.	Kyshtym Reprocessing Plant, USSR (now Russia), 1957
5 Accident with Off-Site Risk	<i>Limited Release:</i> Likely to require partial implementation of planned countermeasures	Severe damage to reactor core or radiological barriers	<ul style="list-style-type: none"> External release of radioactive material (in quantities radiologically equivalent to the order of hundreds to thousands of terabecquerels of iodine-131). Such a release would be likely to result in partial implementation of countermeasures covered by emergency plans to lessen the likelihood of health effects. Severe damage to the installation. This may involve severe damage to a large fraction of the core of a power reactor, a major criticality accident or a major fire or explosion releasing large quantities of radioactivity within the installation. 	Windscale Pile UK, 1957 Three-Mile Island, US, 1979
4 Accident Without Significant Off- Site Risk	<i>Minor Release:</i> Public exposure of the order of prescribed limits	Significant damage to reactor core, radiological barriers, or fatal exposure of a worker	<ul style="list-style-type: none"> External release of radioactivity resulting in a dose to the critical group of the order of a few millisieverts.* With such a release the need for off-site protective actions would be generally unlikely except possibly for local food control. Significant damage to the installation. Such an accident might include damage to major on-site recovery problems such as partial core melt in a power reactor and comparable events at non-reactor installation. Irradiation of one or more workers resulting in an overexposure where a high probability of early death occurs. 	Windscale Reprocessing Plant, UK, 1973 Saint-Laurent, France, 1980 Buenos Aires Critical Assy., Argentina, 1983
INCIDENTS 3 Serious Incident	<i>Very Small Release:</i> Public exposure at a fraction of prescribed limits	Severe spread of contamination or acute health effects to a worker	<ul style="list-style-type: none"> External release of radioactivity resulting in a dose to the critical group of the order of tenths of a millisievert.* With such a release, off-site protective measures may not be needed. On-site events resulting in doses to workers sufficient to cause acute health effects and/or an event resulting in a severe spread of contamination (for example, a few thousand terabecquerels of activity released in a secondary containment where the material can be returned to a satisfactory storage area). Incidents in which a further failure of safety systems could lead to accident conditions, or a situation in which safety systems would be unable to prevent an accident if certain initiators were to occur. 	Vandellós, Spain, 1989
2 Incident		Significant spread of contamination or overexposure of a worker	<ul style="list-style-type: none"> Incidents with significant failure in safety provisions but with sufficient defense in depth remaining to cope with additional failures. These include events where the actual failures would be rated at level 1 but which reveal significant additional organizational inadequacies or safety culture deficiencies. An event resulting in a dose to a worker exceeding a statutory annual dose limit and/or an event which leads to the presence of significant quantities of radioactivity in installation in areas not expected by design and which require corrective action. 	
1 Anomaly			Anomaly beyond the authorized regime but with significant defense in depth remaining. This may be due to equipment failure, human error, or procedural inadequacies.	
DEVIATIONS 0 Below Scale		No safety significance	Deviations where operational limits and conditions are not exceeded. Examples include: a single random failure in a redundant system, spurious initiation of protection systems without significant consequences, leakages within operational limits.	

* The doses are expressed in terms of effective dose equivalent (whole body dose). Those criteria where appropriate can also be expressed in terms of corresponding annual effluent discharge limits authorized by National authorities.

Evaluating Consequences of Malevolent Acts

In the end, what must be recognized is that while it has been fairly easy (if not always transparent) for policy makers to issue target theft categorizations using a variety of attributes such that acceptable levels of protection can be established, that has not historically been the case for radiological sabotage. Furthermore, it would appear that support in the form of some type of safety assessment is required to resolve the issue. As noted by INFCIRC/225/Revision 5 [3], Paragraph 5.5:

- “...the State should consider the range of radiological consequences that can be associated with all its nuclear facilities and should appropriately grade the radiological consequences that exceed its limits for unacceptable radiological consequences in order to assign appropriate levels of protection.”

Intrinsic Security

Applying methods for achieving “intrinsic” security may help to increase margin and robustness against future changes in the threat. See Other SeBD Principle: Achieve inherent or “intrinsic” security (below).

One of the key areas of Security by Design is accommodating possible changes in the threat during the lifecycle of the facility, which may extend 60 to 80 years. There are several ways to do this, applicable to past or current generation reactor designs.

Consider the entire range of natural, accidental, and malicious attacks and look for protection features that are relatively low-cost and address key weaknesses. As a timely example, if the designers of Fukushima Daiichi nuclear plants had considered a range of higher tsunami wave heights, they would have recognized some ways to protect the backup generators. As a security example, consideration of a wide number of aircraft terrorist scenarios before 9/11/2001 would have identified hardening of the cockpit door as a cost-effective solution that would counter a wide range of scenarios.

A design best practice is to leave room or capacity in the facility design to allow for future additions to the security system, e.g., to provide capacity for adding sensors, additional delay features, or additional response capabilities if the threat increases.

The NRC Policy Statement on the Regulation of Advanced Reactors (dated October 14, 2008) [57] contains a number of concepts that can be applied to current reactor designs, including:

- Designs that include considerations for safety and security requirements together in the design process such that security issues (e.g., newly identified threats of terrorist attacks) can be effectively resolved through facility design and engineered security features, and include mitigation measures reduce reliance on human actions.
- Designs with features to prevent a simultaneous loss of containment integrity (including situations where the containment is by-passed), and the ability to maintain core cooling as a result of an aircraft impact, or identification of system designs that would provide inherent delay in radiological releases (if prevention of releases is not possible).

- Designs with features to prevent loss of spent fuel pool integrity as a result of an aircraft impact.
- Designs with features to eliminate or reduce the potential theft of nuclear materials.
- Designs that emphasize passive barriers to potential theft of nuclear materials.

Design of an Intrinsically Secure System

The following principles embody the characteristics of intrinsic security:

- **Defense-in-Depth**
Adversaries must be forced to defeat a number of security features in sequence before accomplishing their goal. These security features should be independent, and require different adversary toolsets, skills, and actions to overcome.
- **Resiliency**
The system must be designed so that security effectiveness remains high in the event of failures of single or even multiple parts of the system—whether through natural events or malicious attack. As successive portions of the system are lost, security effectiveness should degrade slowly and predictably.
- **Lifecycle Security**
Security requirements must be considered throughout the entire lifecycle of the system, including design, production, operation, maintenance, and eventual retirement. Flexibility must be built into the system to ensure security is preserved as threats change over the course of the system lifecycle. Security needs over the course of the lifecycle of the individual security components and of the assets being protected must be considered.
- **Balanced Protection**
Security must be equally effective and robust along all possible adversary attack vectors and across all security domains (physical, cyber, personnel, etc.). The security design must exhibit no “weak links”.
- **Management of Trust**
Trust and privileges extended by the system must be actively managed to limit security threats—particularly from insiders. The least amount of privilege should be given to entities to allow them to perform their functions and nothing else; privileges should be separated when appropriate, and reluctance to trust should be built into the system.
- **Security-by-Default**
The system must, under normal operation, be in a secure state, and only be required to change to a less-secure state infrequently and unusually. Under failure of the system or any of its components—whether through a natural event or malicious attack—the system must transition to the most secure state possible.

- **Leverage**

The system must, whenever possible, leverage immutable laws of nature against adversaries. Fundamental laws of physics, factors in the surrounding environment, and other aspects of the world that adversaries cannot change can be leveraged to increase the difficulty of the adversary attack, increase the time required, or render the asset inoperable, unusable, or significantly less attractive to the adversary.

Without these principles, systems could potentially be designed with security as a primary requirement that is built in from the beginning (i.e., the first two components of “intrinsic security” as we have defined it) but still result in poor security performance. Whenever possible, designs should take advantage of first principles (those associated with the laws of physics) such as radiological, chemical, and physical properties that can be leveraged for security.

Examples of Intrinsic Security

Consideration might be given to the following in security design:

- Opportunities for reducing access points and those who require access.
- Consolidation or distribution of assets, depending on the mission.
- Delay and shielding mechanisms integrated into the construction of walls, doors, and ceilings.
- Closed network systems for mission-critical work separate from administrative systems, and separate from control networks and operational networks.
- Golden copies of trusted software upgraded only after thorough testing to assess impacts and recovery modes.
- Operational security considerations for doorway and window placements.
- Redundancy and recovery mechanisms to ensure failure in a secure mode.

Siting criteria for the facility can also have an impact. Intrinsic security considerations include providing extended detection fields, close proximity to response services, and the ability to withstand abnormal events such as natural disasters or utility construction workers cutting power or communication lines. Crime statistics, neighbors, and visibility of mission criticality should all be reviewed.

It is important to note that there are advantages and disadvantages to most intrinsic security features. For example, some intrinsic security features carry increased system costs or safety risks. Underground facilities can reduce the opportunities for an attack and may make systems more earthquake resistant, but could make it difficult to evacuate or to fight a fire if needed. The location of a facility may enhance security by providing opportunities for wide-area monitoring for early detection and longer interdiction times. However, if response is not site-based, remoteness can delay interdiction. Providing redundant systems can increase mission security, but carry an additional cost since they must also be independent

to ensure no single points of failure. Co-location of primary and secondary systems can minimize the need for additional physical security controls, but can provide single attack vectors.

Flexibility

Because the 3S disciplines need to be intrinsic to the facility design for best effectiveness, and because the design needs to consider changes in conditions over the 60-80 year lifetime of a facility, it is important to be flexible in design and allow for changes over decades of time.

E.4 Topical Area: System Engineering Principles

View the PPS from a lifecycle perspective

Pre-project Considerations during the Scope and Planning Phase

The physical protection objectives and the design basis threat are fundamental to a PPS design. Defining the objectives and threat occur early during the Scope and Planning phase, and are pre-project activities. Facility grading is also important, to the extent that it can be accomplished before the project. To the extent practical, when the State evaluates its readiness and intent to build a NPP or NF, the physical protection experts should provide consultancy to ensure the necessary and sufficient information for later PPS design is available and clearly articulated.

Development of the NPP/NP lifecycle timeline is also a Scope and Planning phase activity. The IAEA Milestones documents [1], [2] for a nuclear power project discusses in detail the pre-project activities and provides insight into the project, transition to operations, and the operational timeframes. As a general statement, the IAEA offers that the lifecycle, including decommissioning and dismantlement, could be approximately 100 years.

During this phase, discussions can begin on prioritizing potentially competing 3S requirements. The prioritization process should occur in a systematic, consistent, and auditable manner allowing assurance to the competent authority that the NPP/NF conforms to the State's laws, regulations, and environmental criteria.

Facility grading and prioritization can be evaluated using a security risk assessment approach which incorporates the considerations covered in Appendix B, Evaluating security Risk Assessment Factors, and in Appendix C, Security Risk Management.

Synergy between Safety, Safeguards, and Security

It is important to realize that the security design process is one part of a larger facility design process, done within a larger regulatory framework that also considers safety and safeguards—the overall 3S process.

Security is a cross-cutting function and all aspects that potentially impact security must be considered during the design process. Although we mostly refer to 3S, this would actually include physical security,

MC&A, International and domestic safeguards, process design, operations, safety, cyber security, reliability, and sustainability.

Much work needs to be done on developing tools, strategies, and practices for integrating safety, security and safeguards requirements into the overall facility design process, as well as demonstrating that the integrated design process improves overall effectiveness and reduces lifecycle costs of the facility design.

As mentioned earlier in this document, there are two key concepts to keep in mind in achieving a successful physical protection system implementation:

- Security requirements should be considered as early in a facility design process as possible.
- A structured systems engineering process should be used for the design and evaluation of a physical protection system.

Since this handbook focuses on security by design, the physical protection design team should concentrate on specifying the security requirements as completely as possible and, and equally importantly, on identifying interface points with the larger design process.

- Within the structured systems engineering process (see the INCOSE systems engineering handbook [37]), as a standard first step in the facility design process, a formal requirements process should be used to cover safety, security, and safeguards (3S).
 - Different level of requirements can be stated (international and national regulations down to detailed design requirements), and complementary and conflicting requirements can be identified.
 - The physical protection design team should focus on specifying the security requirements as completely as possible, and on identifying key interfaces to requirements in the other areas.
- Characteristics of the facility and its *mission* should also be considered in terms of how they could contribute to security. For example, in some recent work, process monitoring measurements seem to provide the earliest indicator of issues in a reprocessing plant. [58]
- While there are a variety of quantitative evaluation tools (e.g., safety codes, SAVI, Separations Safeguard Performance Model), their outputs are not integrated but could be, and efforts are currently underway between Material Control and Accountability (MC&A) and physical security. A good example of integration across areas is the 2008 IAEA Implementation Guide for Preventative and Protective Measures against Insider Threats [50].

To identify possible areas for synergy, one practice is to create a crosswalk table to compare security features with safety and safeguards requirements/features. Another approach is to examine surrogate documents such as DOE STD 1189-2008 [9] to guide security integration with safeguards design.

DISTRIBUTION

[List in order of lower to higher Mail Stop numbers.]

1	MS3161	C. Jaeger	6833
1	MS3161	S. Ortiz	6833
1	MS3161	C. Scharmer	6833
10	MS3161	M. Snell	6833
1	MS0899	Technical Library	9536 (electronic copy)
1	MS0899	RIM-Reports Management	9532 (electronic copy)



Sandia National Laboratories