SAND2013-5170C

Security-By-Design Handbook

International Conference on Nuclear Security
Enhancing Global Efforts
Vienna, Austria
1-5 July 2013

Mark Snell, Calvin Jaeger, Sabina Jordan and Carol Scharmer
Sandia National Laboratories

Koji Tanuma, Kazuya Ochiai, and Toru Iida
Japan Atomic Energy Agency

SAND XX

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.

NNSA National Nuclear Security Administration

JAEA

Sandia National Laboratories

Outline

- Security-By-Design (SeBD)
  - What is it and What is the value?
  - Factors contributing to SeBD
- SeBD Handbook Structure
- Strategies for Achieving SeBD
- SeBD Principles and Practices
- Summary

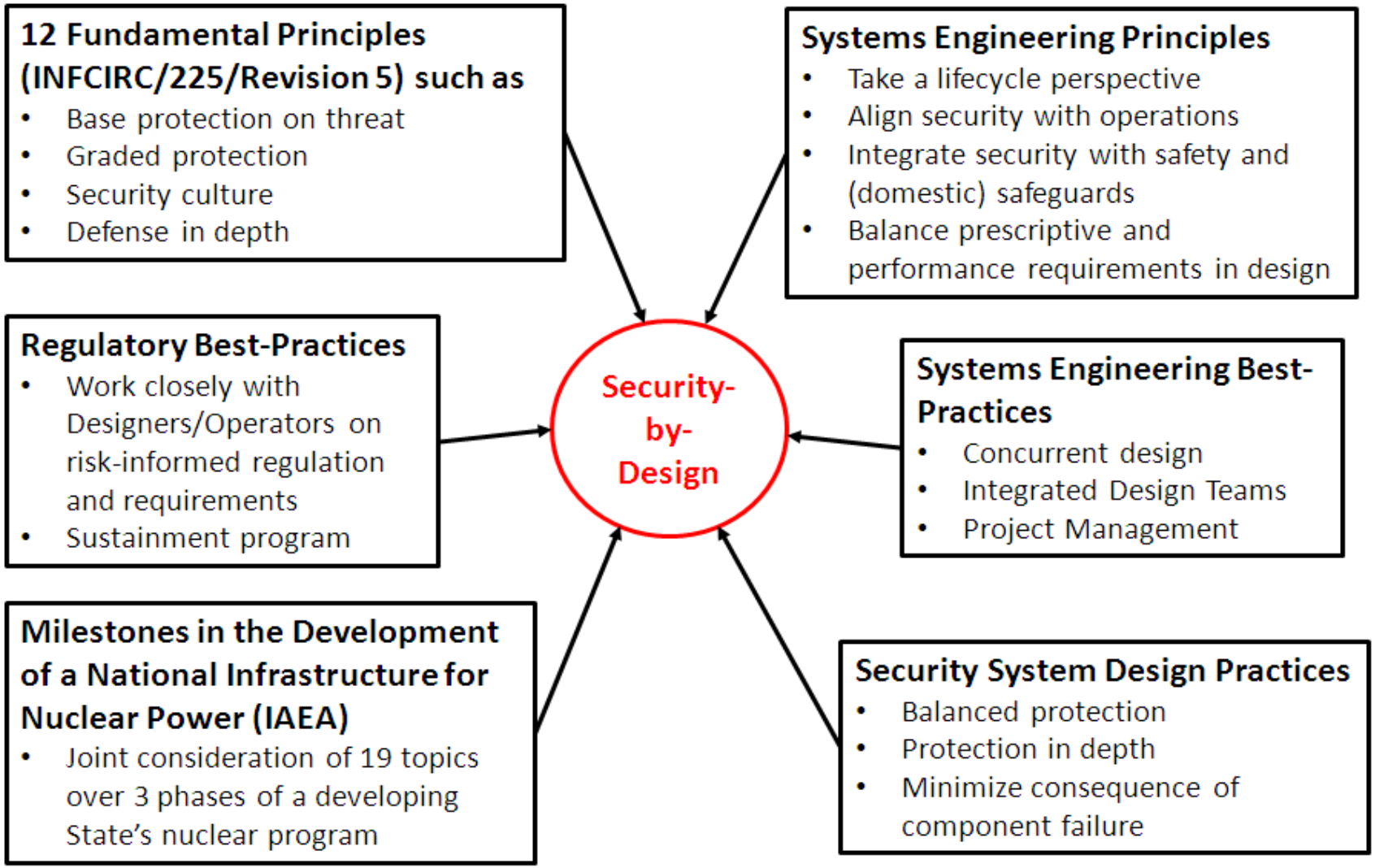
What is Security-By-Design (SeBD)

- Definition of SeBD: System-level incorporation of PP into the nuclear facility to minimize the risk of theft and sabotage through features inherent to the facility design
- Basic Idea: Incorporate PP into facility designs from the beginning rather than design the physical protection system (PPS) *after* the facility design is set
- Intent: Design the nuclear facility so as to provide an adequate level of PP throughout the lifetime of that facility
  - In a cost effective fashion
  - Without negative impacts on operations, safety and safeguards

What is the value of following SeBD?

- SeBD offers a systematic approach to addressing:
  - Late involvement of security in the design process.
  - PPS designs based on no threat or only on consideration of the current threat
  - Lack of proper integration between security and operations, safety, and safeguards, leading to inefficiencies.
  - Weaknesses in governance and organizational structures.
  - Little or no consideration of the facility lifecycle.
- SeBD offers opportunities to help reduce costs and for the physical protection system to remain effective over time.
- SeBD allows the protection system to more easily adapt to meet the evolving threat.

Factors contributing to Security-By-Design



SeBD Handbook Structure

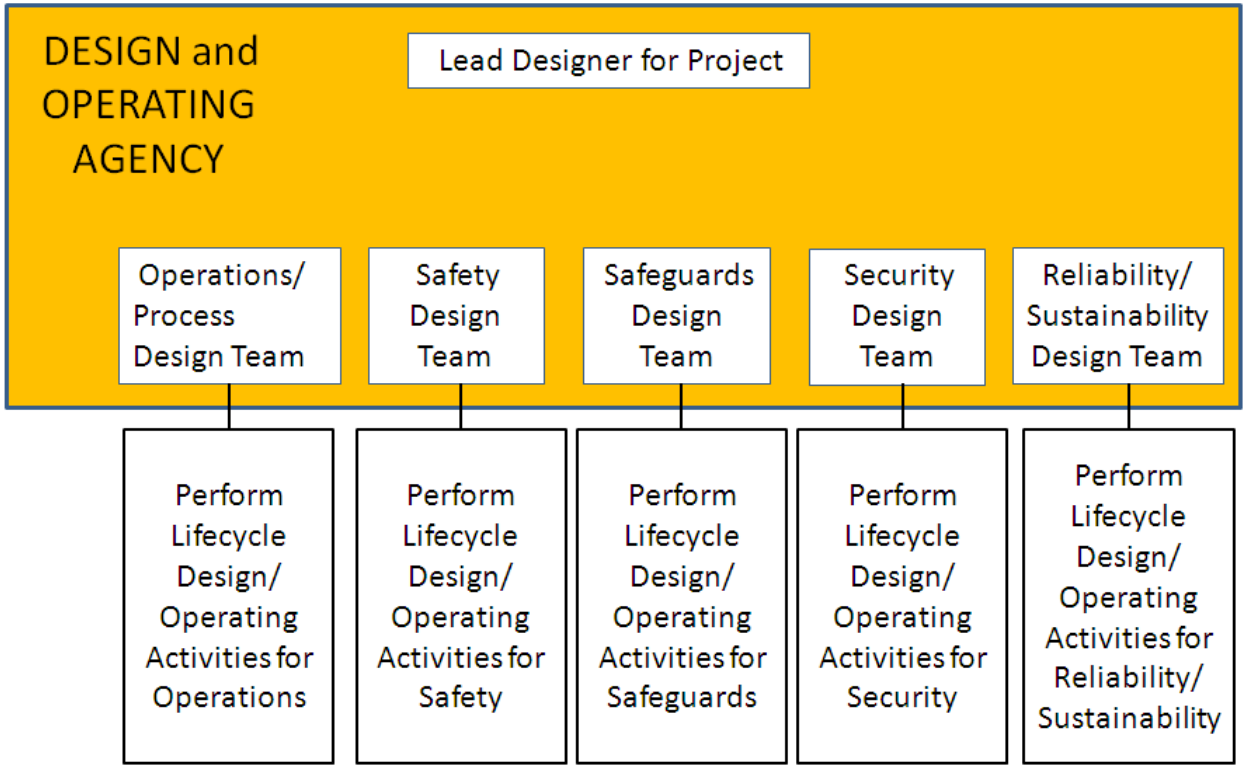
- Section 2 provides an overview of the SeBD framework and discusses the value of using that framework in the design process
- Section 3 describes an approach or strategy for implementing SeBD within the context of the recommendations found in INFCIRC/225/Revision 5 and the Milestones documents
- Section 4 describes Principles and Practices for achieving SeBD
- Section 5 describes in some detail how the SeBD framework has been and can be applied
- Appendices provide more detail on the SeBD generic process design process, evaluating security risk assessment and security risk management and more discussion on the principles and practices grouped into topical areas

Strategy for Achieving SeBD

- **Integrated Design Team**: Incorporation of a physical protection team (PPT) within the context of the overall design team;
- **Risk Informed Design**: Use of a risk-informed design decision-making process that addresses threat, vulnerability, and consequence;
- **Facility Design/Operations Lifecycle**: Use of a structured lifecycle process for the integrated design team, where details are provided for the activities that the PPT needs in order to achieve SeBD; and
- **Principles and Practices**: Discussion of a set of physical protection principles and practices, how these practices can be implemented, and a description of how these principles and practices can be integrated into the lifecycle process.

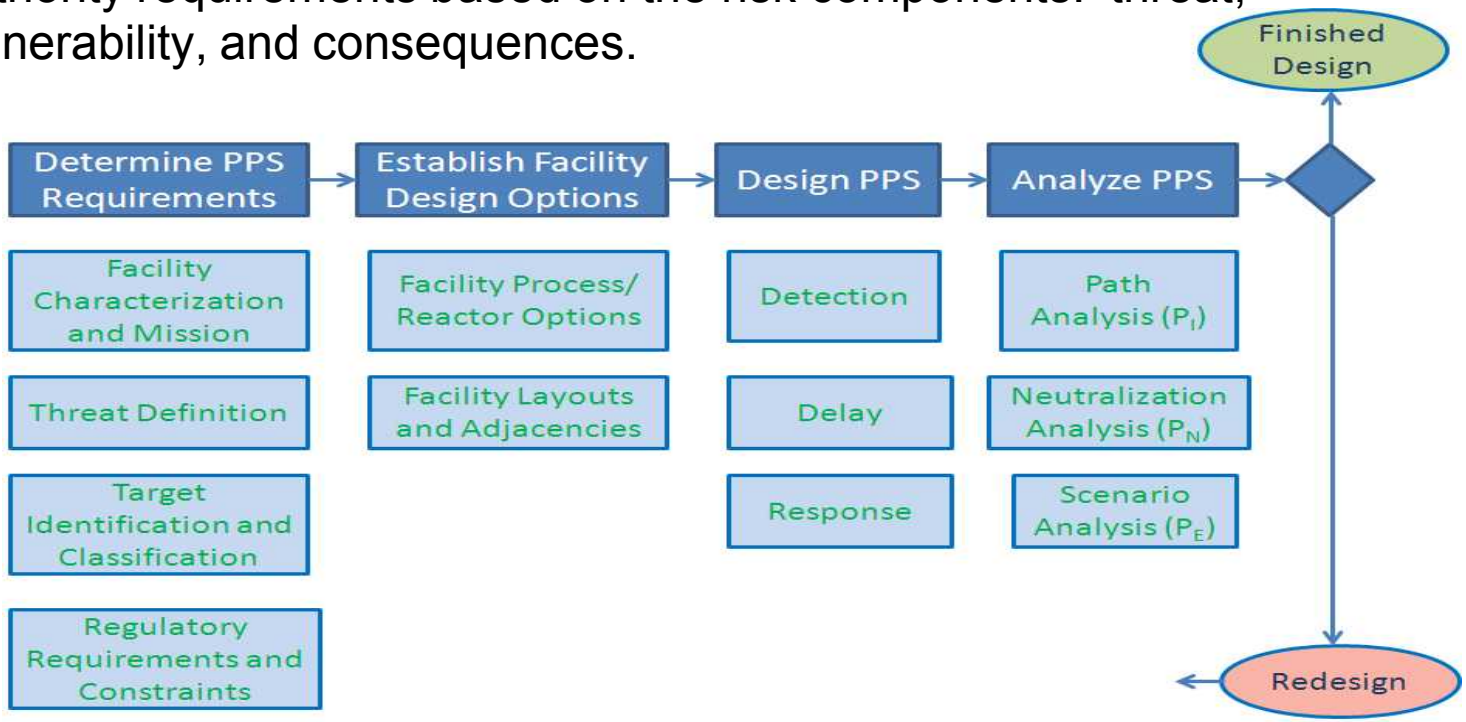
Integrated Design Team

- 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 nuclear facility lifecycle.

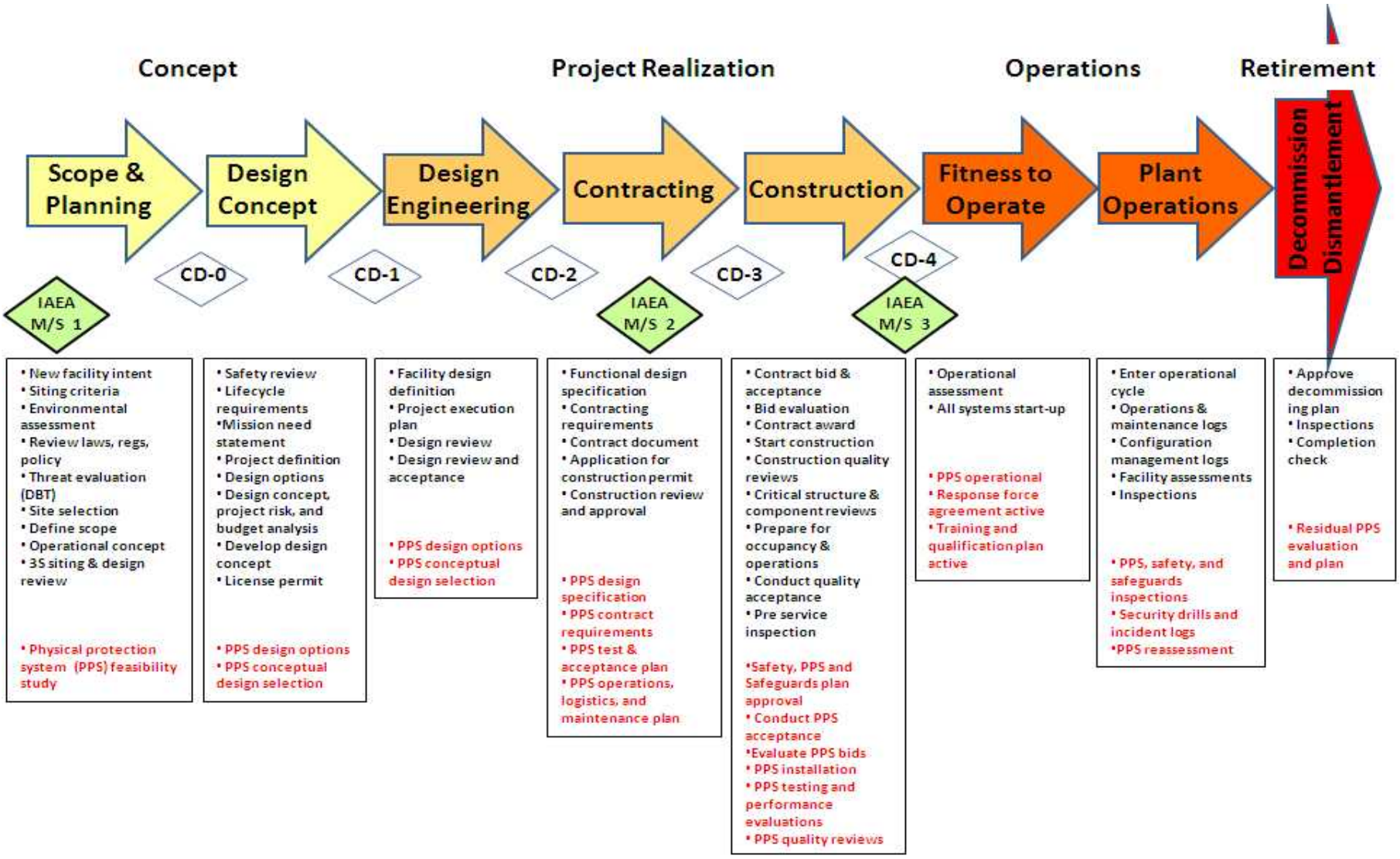


Risk-Informed Design

- "Risk informed" refers to decision-making processes that includes risk as one of several metrics considered in making the decision(s). The process has two major components:
  - The process for design and evaluation of the physical protection system within the context of a facility design.
  - A risk-informed approach to analyzing the design against competent authority requirements based on the risk components: threat, vulnerability, and consequences.



Facility Design/Operations Lifecycle



SeBD Principles and Practices

- The Handbook describes the principles (”what’) and their associated practices (“how’):
  - The 12 Fundamental Principles (A-L) of Physical Protection of Nuclear Material and Nuclear Facilities.
  - Other principles:
    - Inherent/intrinsic security
    - Lifecycle perspective
    - Concept of operations
    - Synergy of 3Ss
    - Design-in sustainability
    - Balance between prescriptive and performance requirements
    - Proven engineering
    - Proven project management
    - Proven operational planning
    - Systems engineering
    - Effective communications
    - Project/operations experience

Summary

- We discussed:
  - What is SeBD
  - The value of SeBD
  - Factors contributing to SeBD
- Structure of the SeBD Handbook
- Strategy for achieving SeBD
- Facility Design/Operations Lifecycle
- SeBD Principles and Practices

Security-by-Design Handbook, SAND2013-0038, January 2013