SAND2010-4405P

Development of a Security-By-Design Handbook

51st Annual Meeting of
Institute of Nuclear Materials Management (INMM)
Baltimore, MD
July 15, 2010

Mark Snell and David Olson
Sandia National Laboratories

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

SAND2010-XXXXC

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: What is it and Why?
- Project Overview
- Description of Work to Date
  - Principles and Practices
  - Generic Design Process
- Planned Work
- Summary

Security-By-Design – What is it?

- Security-by-design: the system level incorporation of the physical protection system (PPS) into a new nuclear facility resulting in intrinsic security.
  - PPS minimizes the risk of malicious acts resulting in nuclear material theft or sabotage and facility sabotage.
- For existing nuclear facilities, the PPS may be integrated into the facility;
  - Post construction integration may not achieve the efficiency and effectives of system level design.

Project Overview

- Objective
  - Develop a Security-By-Design handbook for future facilities
- Intended users
  - Current physical protection designers
  - The next generation of physical protection designers
  - Facility designers in emerging countries
- Related Goal
  - Develop a Security-By-Design information dissemination plan
- Project is sponsored by National Nuclear Security Agency (NNSA) between Sandia National Laboratories (SNL) and Japan Atomic Energy Agency (JAEA)

Security-By-Design Principles and Practices for the Facility Lifecycle

Systems Principles
- Lifecycle Perspective
- Consider All Operating Conditions

CPPNM Fundamental Principles
- Responsibilities (State, Competent Authority(CA), Licensee)
- Base Physical Protection on Threat
- Graded Protection
- Security Culture, Confidentiality
- Quality Assurance, Contingency Plans

Safety/Domestic Safeguards/Security
- Principle: Balance in design
- Principle: Balance Detection, Delay, Response functions
- Practice: Establish priorities

Security-By-Design

Systems Engineering Practices
- Concurrent Design
- Project Management
- Use of Trade-off Studies

Regulatory Best Practices
- Lessons-learned
- Adopt commonly-used guides and standards
- Maintain Close, Honest Relationship with CA

Security Design Practices
- Defense in Depth
- Measure effectiveness against threat

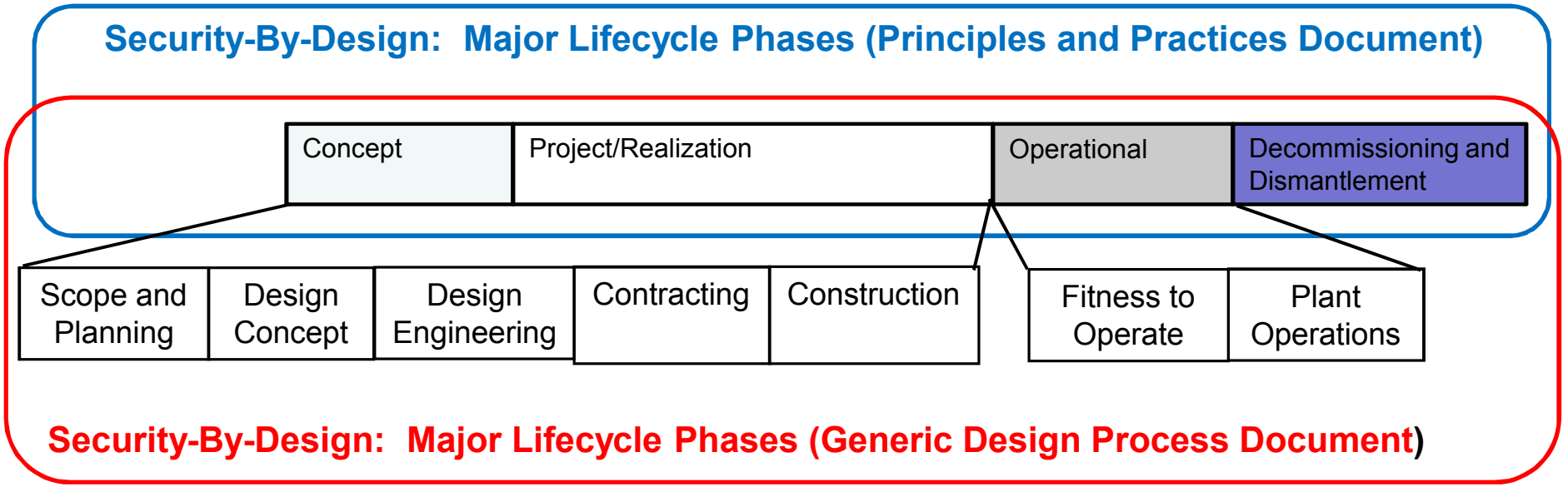
Entire Lifecycle, Realization, Operational

Collection of Insights for Security-By-Design

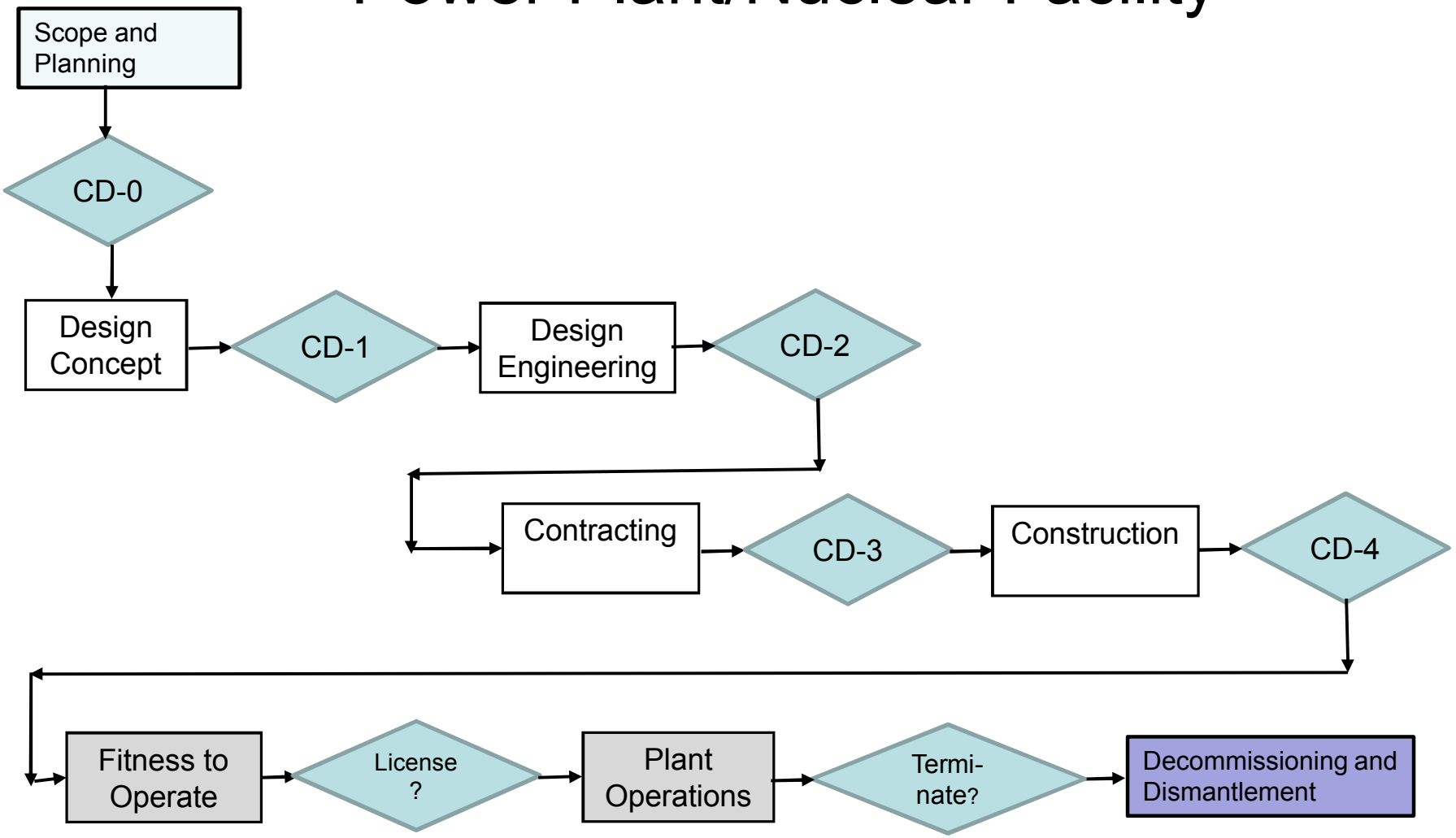
- Realization (Design/Build)
  - Principle: Treat security as a key function during design
  - Principle: CA should balance prescriptive and performance-based security requirements and have mechanisms to relax prescriptive requirements,
  - Practice: Employ Intrinsic Security design methods
- Operational
  - Ensure adequate staffing, funding and independence
  - Monitor system performance and test

Entire Lifecycle,
Realization,
Operational

Security-By-Design Lifecycle Phases for the Purposes of the Generic Design Process



Notional Lifecycle for New Nuclear Power Plant/Nuclear Facility



Iterative Use of Vulnerability Assessments During Lifecycle

Phase	Value of Assessment	Occurs
Scope	Assures principal design requirements are consistent with mission need	CD-0 Project Authorization
Concept	Choose among competing facility and PPS design approaches	CD-1 Design Selection
Design	Optimize facility and PPS design consistent with S3 priorities	CD-2 Design Approval
Construction	Continuous assurance PPS design achieves security objectives	CD-3 Construction
Acceptance	Performance validation of PPS, operators, and response force for entry into operations	CD-4 Acceptance
Operations	Verification PPS performs as designed and remains consistent with threat	Operational Inspections & Assessments
Decommission & Dismantle	Determine residual PPS requirements post operations	

Planned Work

- Document how the principles and best practices can be best integrated into the design process
- Develop a security-by-design handbook
  - What level of knowledge, examples, details
- Develop a plan for getting security-by-design information out to the intended audience
  - Intended audience
  - Best methods to transfer information

Summary

- We described
  - A variety of Security-by-Design principles and best practices
  - A generic design process that addresses the entire facility lifecycle
- Work is progressing to develop a Security-by-Design handbook