SAND2022-8717C

Sandia National Laboratories

A Dynamic, Integrated Approach to Vital Area Identification

Presented by:

Brian Cohn

Presented at The 16th Probabilistic Safety Assessment & Management Conference

U.S. DEPARTMENT OF ENERGY | NNSA

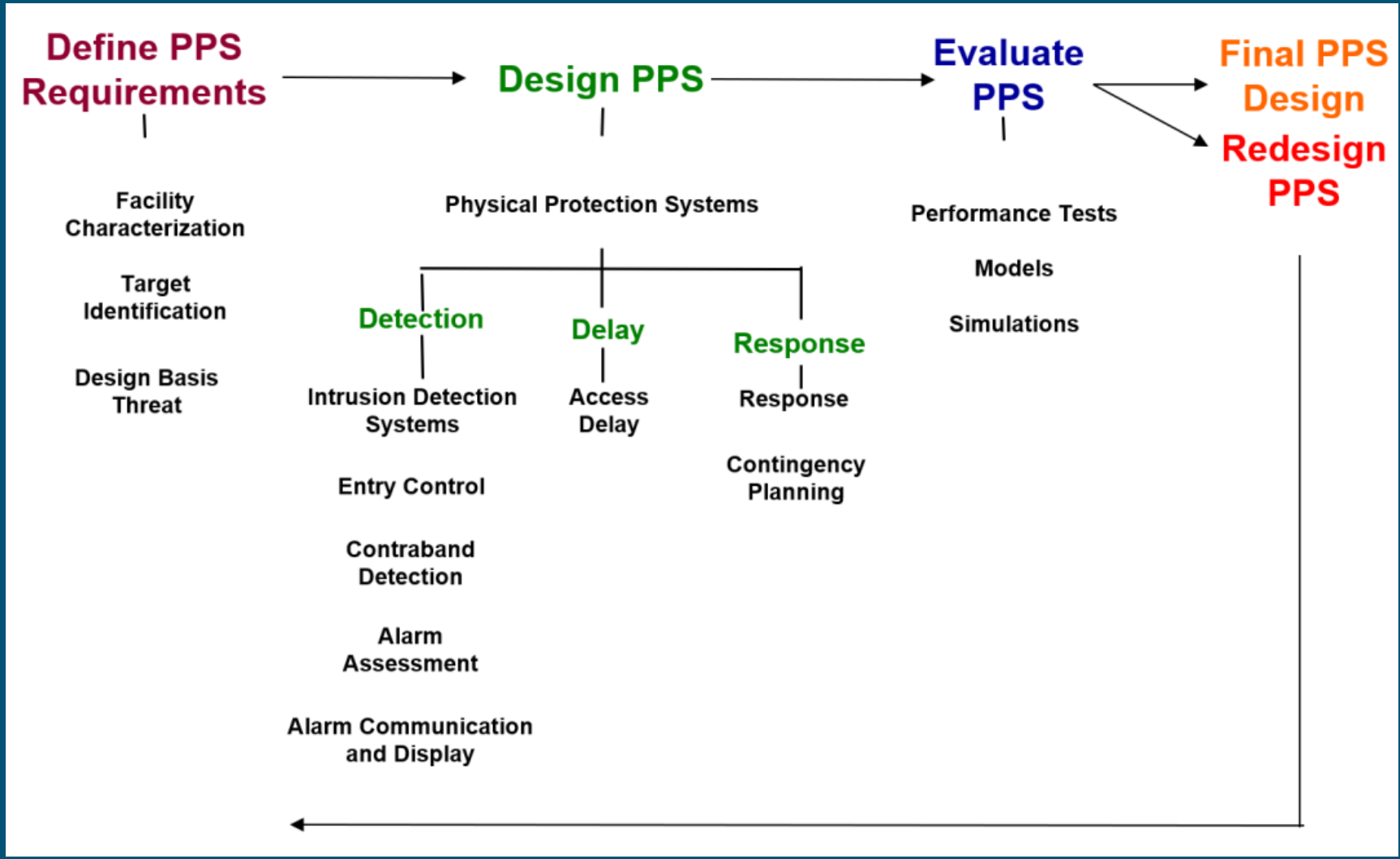
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Introduction

The Design Evaluation Process Outline (DEPO) methodology is widely used for developing physical protection systems (PPSs)

Vital Area Identification (VAI) plays a key role in implementing the DEPO and other PPS design processes



VAI Overview

VAI serves at the foundation for nuclear security analysis

- Based on static fault tree/event tree (FT/ET) analysis to determine vital equipment to protect with the physical protection system
- Vital areas are based on preventing severe core damage from adversary sabotage

Challenges with the VAI structure

- FTs are largely sourced from safety analysis with inbuilt safety assumptions that can be difficult to reappropriate
- VAI implies the instant onset of severe core damage following adversary sabotage of vital equipment
- For some scenarios, vital areas are only sabotage targets for a limited period of time
- Little communication between safety and security risks

Previous Work

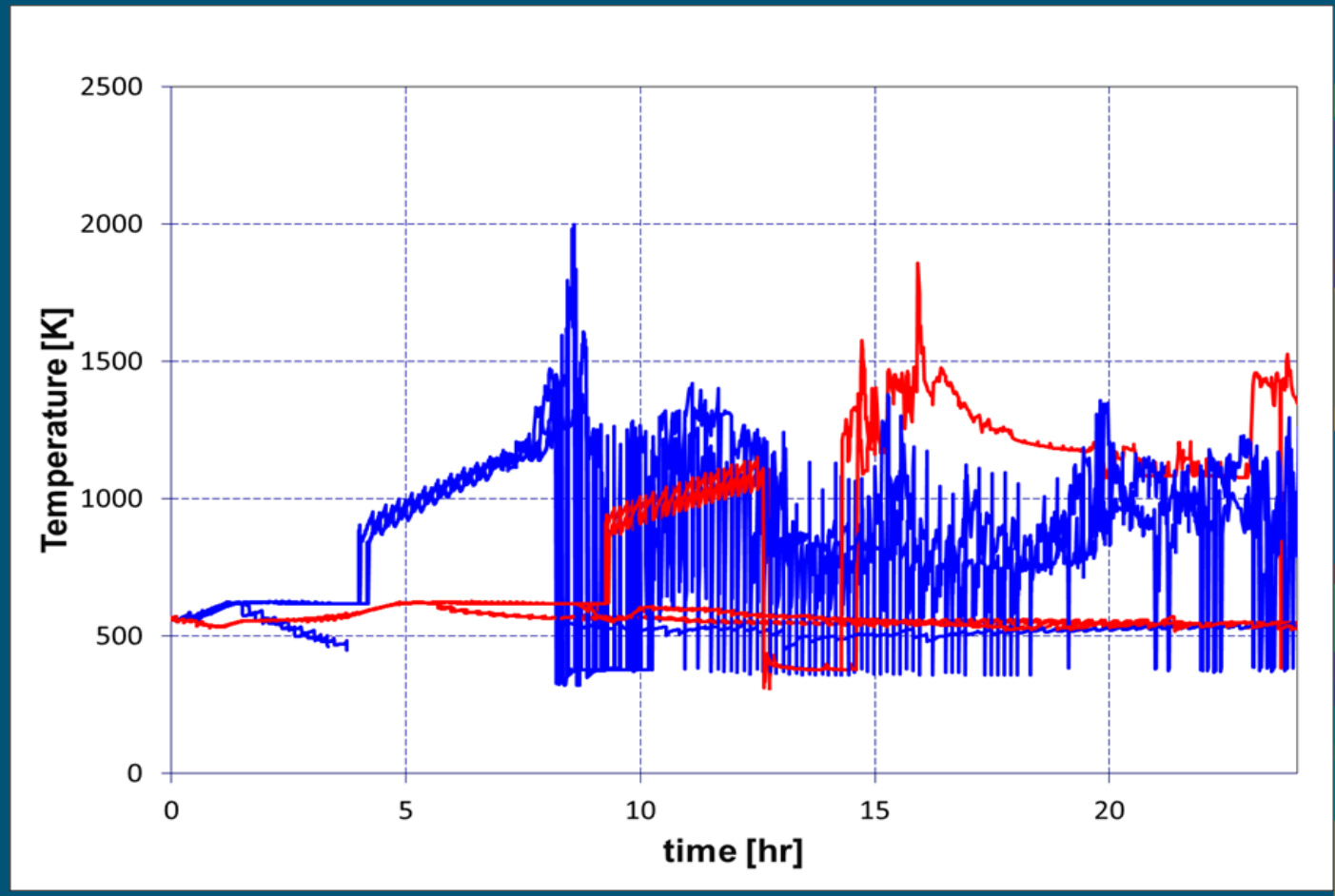
Integrated dynamic safety-security (2S) analysis of a hypothetical LWR

- Connected MELCOR reactor response analysis to security modeling
- Modeled successful sabotage of a complete target set

Case study found strong dynamic elements

- Level of damage from sabotage
- Success of mitigation and recovery actions

Minimal environmental releases



Dynamic Approach to Vital Area Identification

Intent is to use 2S analysis to inform vital areas

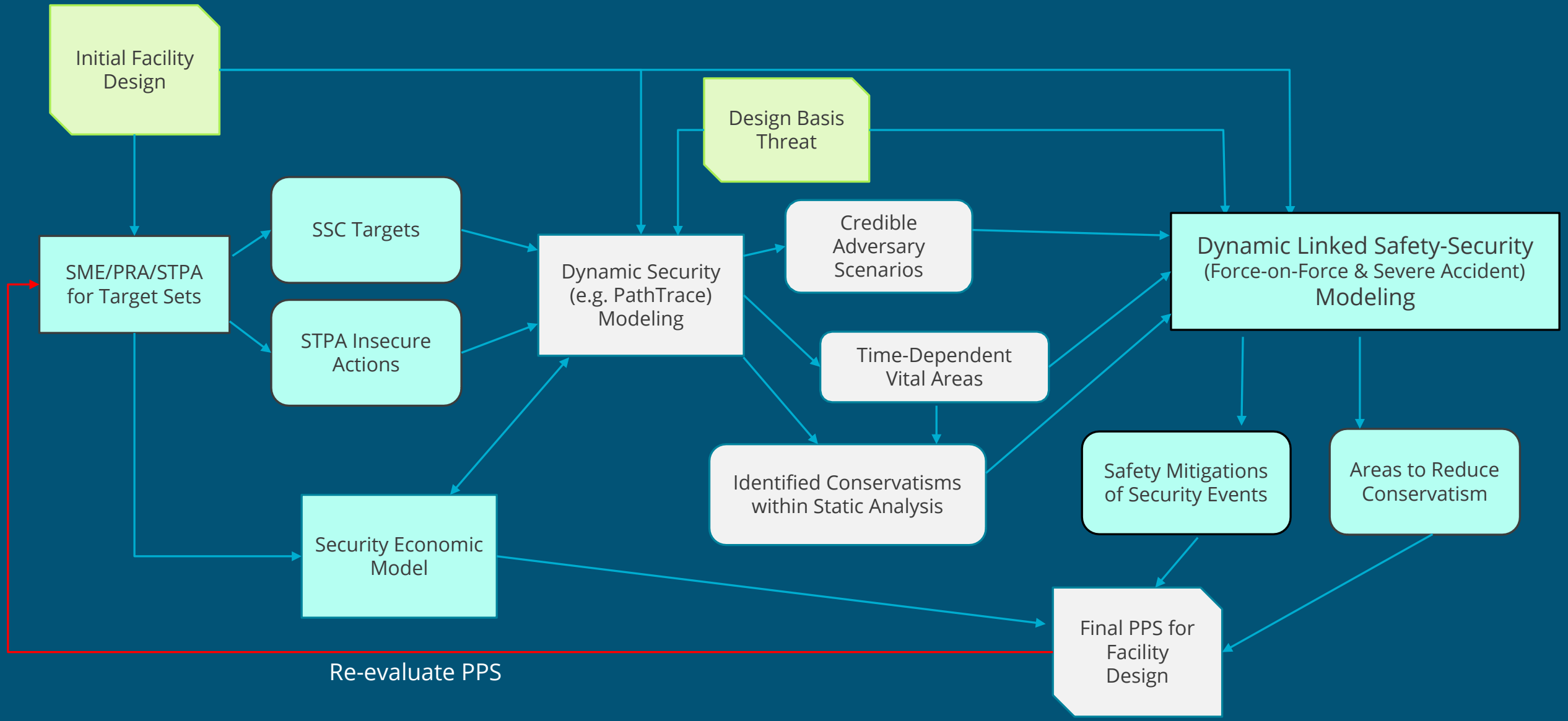
- Identify adversary sabotage activities with associated timing
- Use timings to determine consequences to the reactor

Based on Systems Theoretic Process Analysis (STPA) and Dynamic Probabilistic Risk Assessment

- STPA is effective at systematically identifying systems of concern
  - Poor at prioritizing between systems
- DPRA is effective at determining consequences of scenarios
  - Poor at identifying scenarios of concern

Combined STPA and DPRA analysis can be more than the sum of its parts

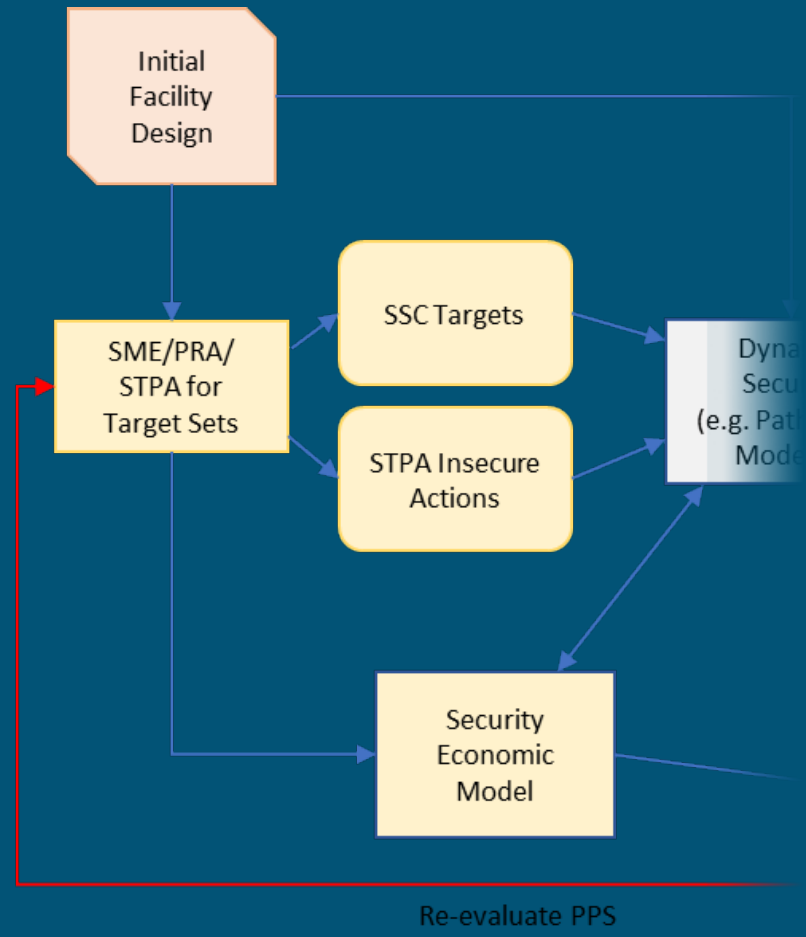
Proposed Dynamic VAI Approach



Phase 1

Purpose of this phase is to generate a comprehensive list of security-relevant systems

- Analysis is not concerned at this stage with the relationships between systems
- List of relevant systems can be obtained from:
  - SME judgment
  - PRA
  - STPA
- Can include passive safety systems and digital controls

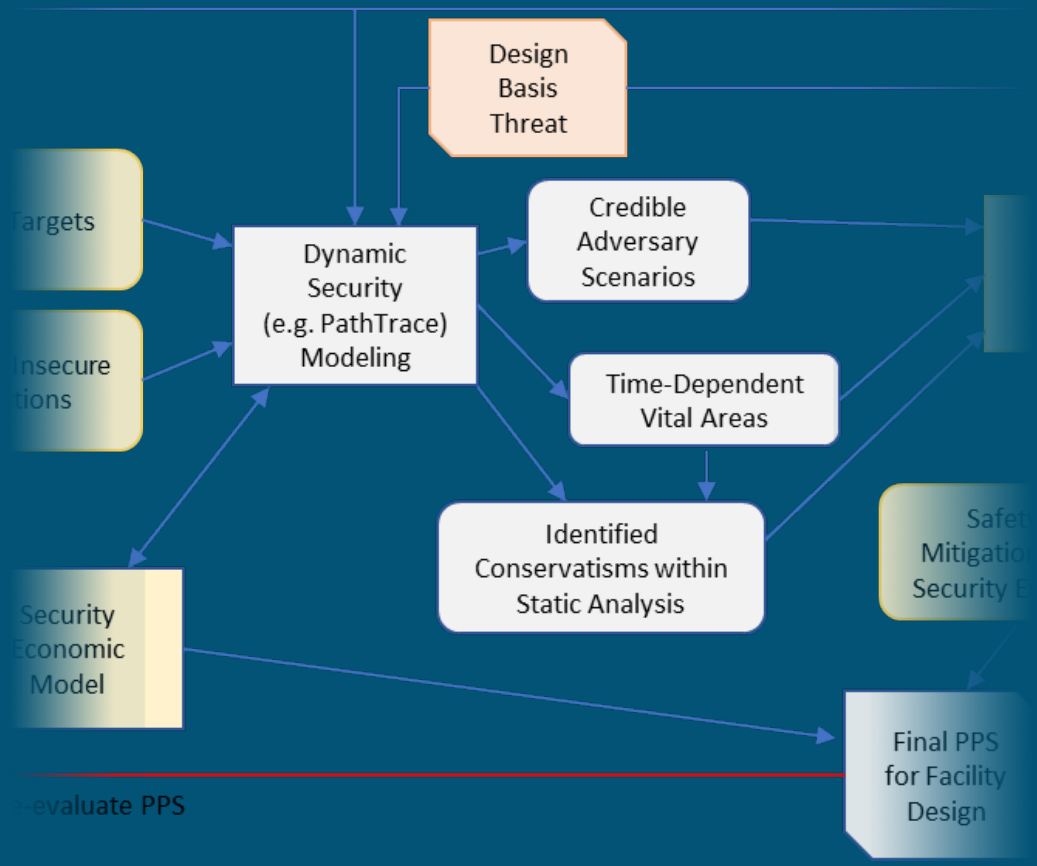


Phase 2

Purpose of this phase is to generate conservative adversary attack timelines

- Dynamic security modeling used to understand the impact of sabotage
  - PathTrace or other timeline model constructed
  - Sabotage timings generated for each permutation of targets
  - Timing information is sent to reactor response model to determine consequences of sabotage
  - Output is a list of credible adversary scenarios

Reactor response strategies not considered in this phase

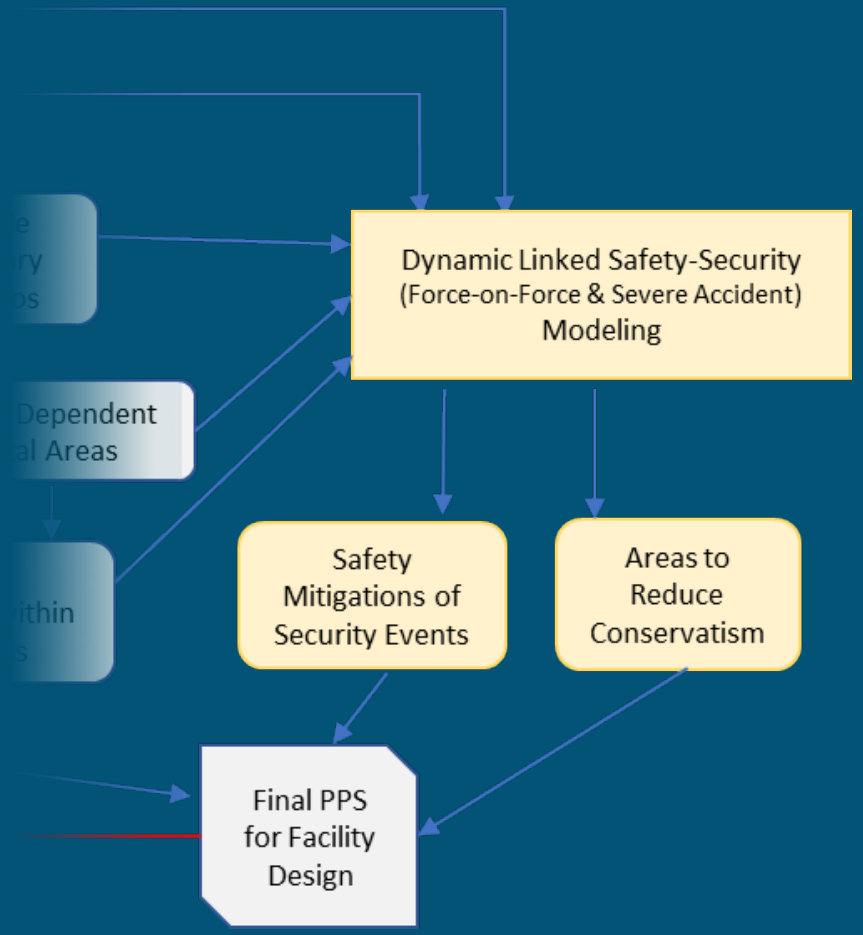


Phase 3

Purpose of this phase is to determine the physical protection system's effectiveness against the credible adversary scenarios

- Credible scenarios are entered into a force-on-force code
- Reactor response model receives information on damage to safety systems and determines appropriate responses
- Operator and response force activities can take the state of the plant into consideration
  - Models mitigating actions
- Analysis can extend beyond core damage to radionuclide release

Similar to the previously described 2S analysis



Proposed Case Study

A case study integrating all three phases has been proposed for analysis

- Uses the hypothetical Lone Pine Nuclear Power Plant
- Previously modeled during 2S analysis

Analysis is limited in scope to modeling the auxiliary feedwater (AFW) system

- Rest of the plant will be modeled, but only consider availability of AFW

Is intended to combine all three phases of the dynamic VAI approach

Considers the success of the reactor despite sabotage to vital equipment

Conclusions

Existing VAI methodologies rely on conservatism to ensure the protection of NPPs

Limitations of static VAI present challenges for advanced reactors

- Reliance on passive safety systems
- Use of digital control systems
- Potential for adversaries to achieve some sabotage of systems

Proposed a dynamic VAI methodology

- STPA to systematically identify critical components
- DPRA to determine dynamic effects of adversary sabotage to components

Case study may be able to determine the effectiveness of the proposed methodology

Questions?