SAND2015-3631C

The Treatment of Blended Attacks in Nuclear Security Effectiveness Assessments

Mark Snell, Sandia National Laboratories,
Joseph Rivers, United States Nuclear Regulatory Agency

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.
SAND2015-

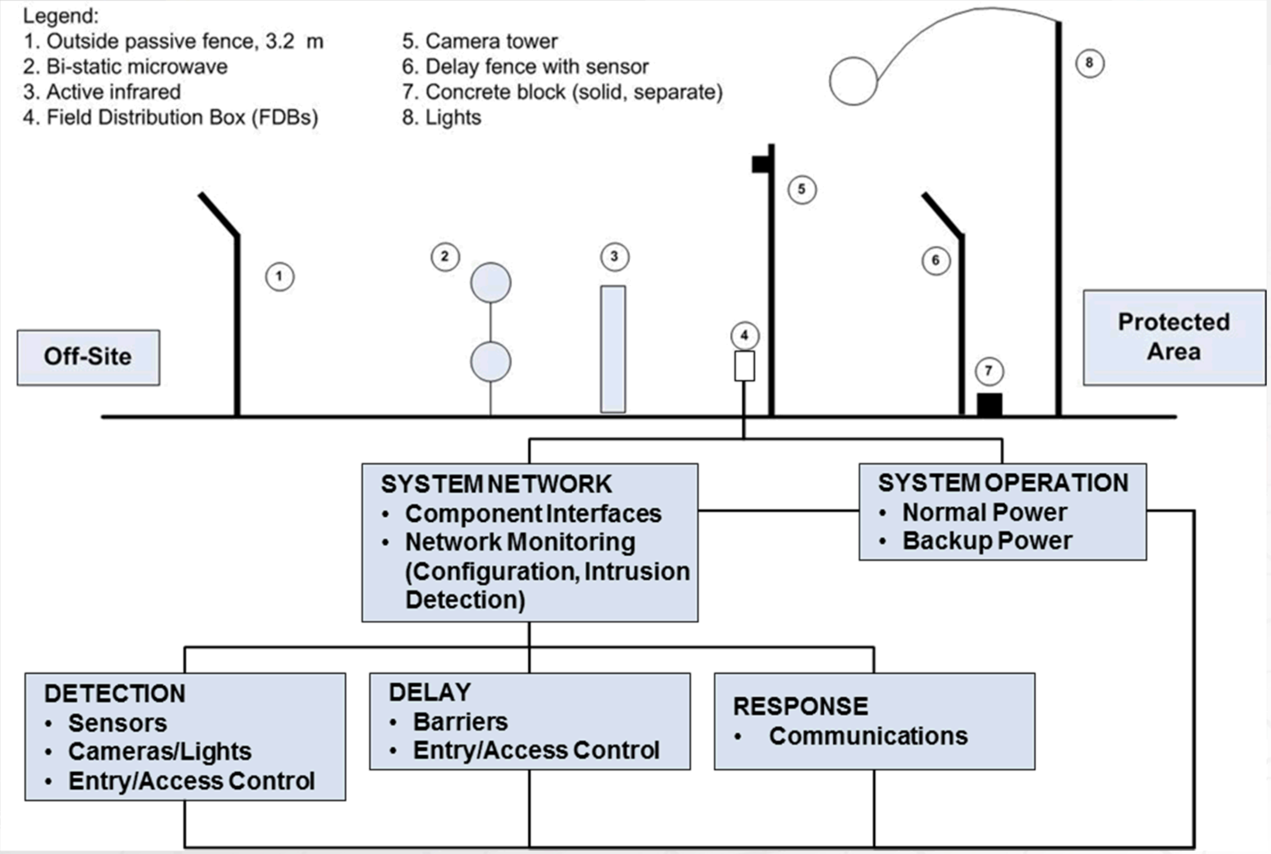
Outline

- Overview of blended attack problem
- Evaluation process for identifying adversary scenarios
- Use of the United States Nuclear Regulatory Commission's Critical Digital Asset (CDA) regulatory approach

Overview of the Blended Attack Problem

- Definition: cyber and information attacks are used to support physical attacks by outsider or insider threats within a Design Basis Threat (DBT)
- Need for a technique that
  - Is consistent with existing techniques, with a minimum amount of additional training
  - Is systematic and produces credible scenarios

Schematic of a Hypothetical Combined Cyber-Physical Protection System



Legend:

1. Outside passive fence, 3.2 m
2. Bi-static microwave
3. Active infrared
4. Field Distribution Box (FDBs)
5. Camera tower
6. Delay fence with sensor
7. Concrete block (solid, separate)
8. Lights

SYSTEM NETWORK
- Component Interfaces
- Network Monitoring (Configuration, Intrusion Detection)

SYSTEM OPERATION
- Normal Power
- Backup Power

DETECTION
- Sensors
- Cameras/Lights
- Entry/Access Control

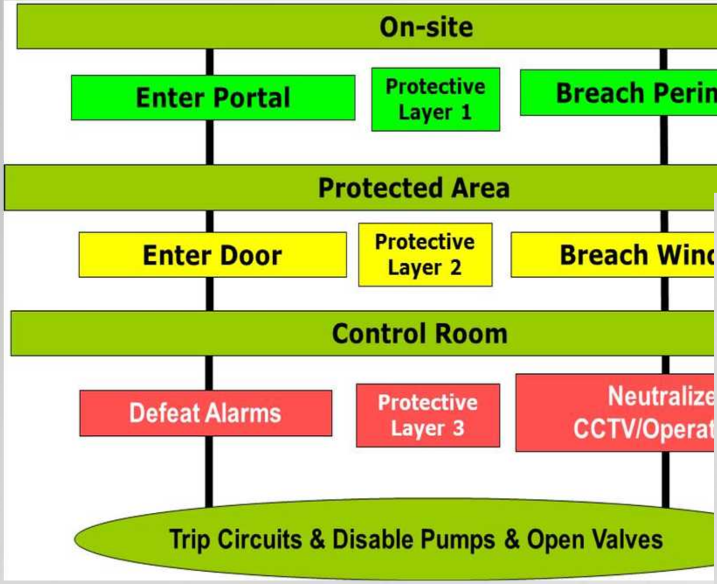
DELAY
- Barriers
- Entry/Access Control

RESPONSE
- Communications

Steps in the Proposed Evaluation Process

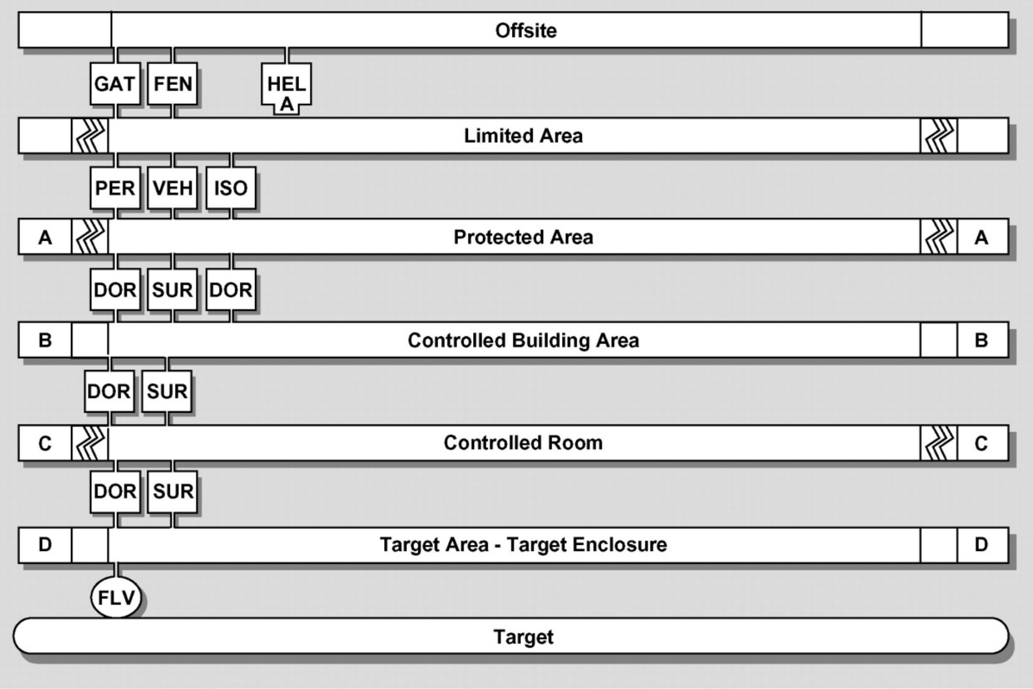
1. Apply current evaluation methods against insider, outsider, and collusion threats
2. Identify critical physical protection system (PPS) elements
3. Apply Cyber Security evaluation techniques to critical PPS elements
4. Combine the Results of the Cyber Security Evaluation with the PPS Evaluation

Current Evaluation Methods: Path/Adversary Action Sequence Networks



Adversary Action Sequence Diagram

Adversary Sequence Diagram

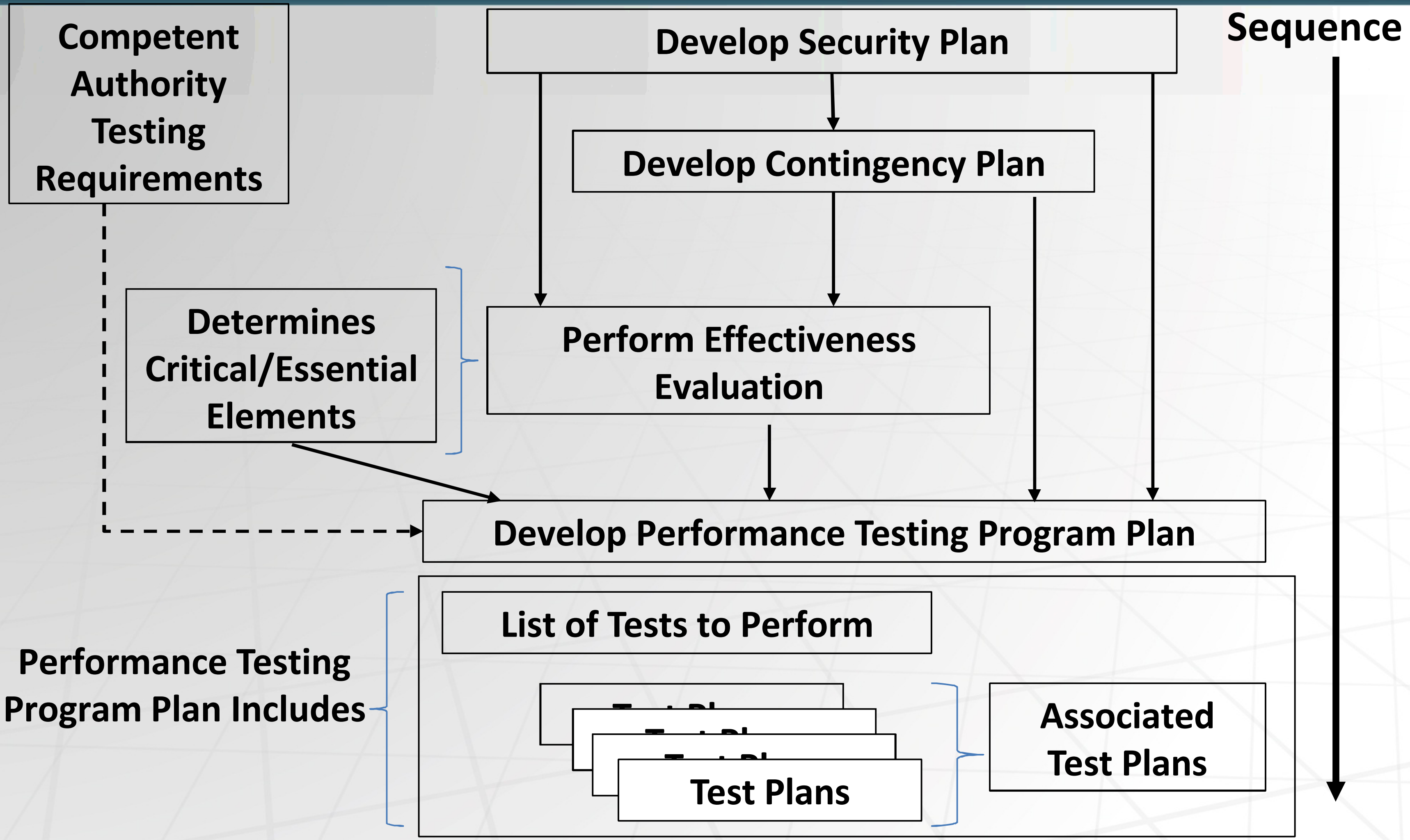


Scenario analysis is also typically performed

Methods for Identifying Critical PPS Elements

- Inspection of the PPS architecture to identify non-redundant, but required systems
- Performance of a conventional collusion analysis for existing insiders colluding with outsiders and determine what PPS measures are most critical
- Review of
  - Performance Testing Program Plans for those elements that are most critical elements to test
  - Contingency plans, including compensatory measures
  - Non-security test plans and quality plans

Site Performance Testing Planning Sequence



Competent Authority Testing Requirements

Develop Security Plan

Develop Contingency Plan

Determines Critical/Essential Elements

Perform Effectiveness Evaluation

Develop Performance Testing Program Plan

Performance Testing Program Plan Includes

List of Tests to Perform

Test Plans

Associated Test Plans

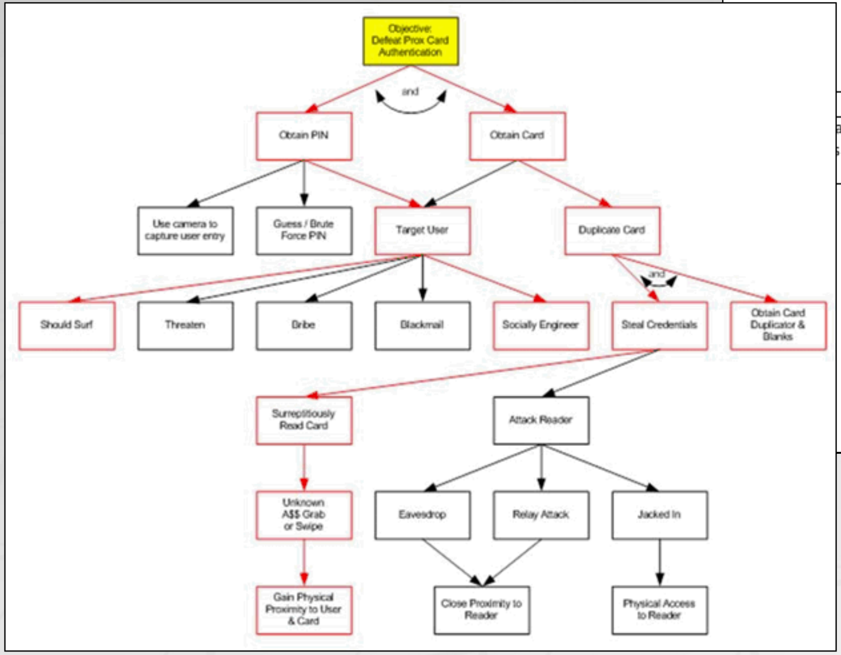
Sequence

Apply Cyber Security Evaluation Techniques to Critical PPS elements

- Existing cyber security assessment techniques to determine which critical PPS elements, if any, can be defeated using cyber-attacks
- Deductive methods such as logic diagrams
  - How can some system failure state be caused?
- Inductive methods based on some adversary action
  - What happens if?...

Two Types of Logic Diagrams

Attack Trees



Objective: Defeat Prox Card Authentication

and

Obtain PIN

Obtain Card

Use camera to capture user entry

Guess / Brute Force PIN

Target User

Duplicate Card

and

Should Surf

Threaten

Bribe

Blackmail

Socially Engineer

Steal Credentials

Obtain Card Duplicator & Blanks

Surreptitiously Read Card

Attack Reader

Unknown A$$ Grab or Swipe

Eavesdrop

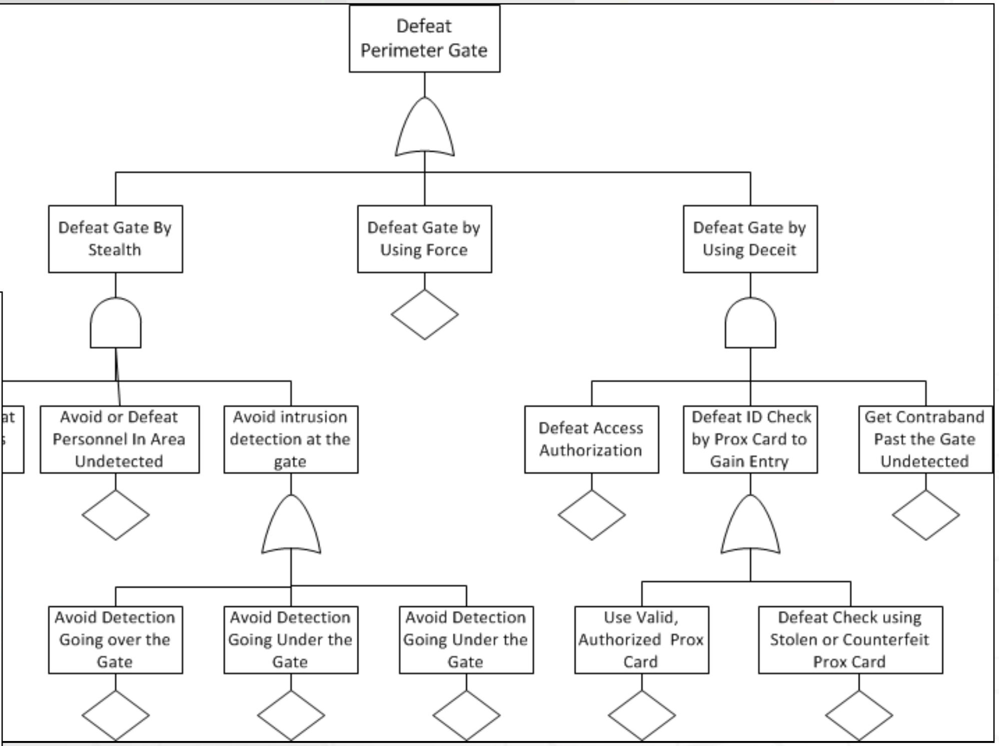
Relay Attack

Jacked In

Gain Physical Proximity to User & Card

Close Proximity to Reader

Physical Access to Reader



Defeat Perimeter Gate

Defeat Gate By Stealth

Defeat Gate by Using Force

Defeat Gate by Using Deceit

Avoid or Defeat Personnel In Area Undetected

Avoid intrusion detection at the gate

Defeat Access Authorization

Defeat ID Check by Prox Card to Gain Entry

Get Contraband Past the Gate Undetected

Avoid Detection Going over the Gate

Avoid Detection Going Under the Gate

Avoid Detection Going Under the Gate

Use Valid, Authorized Prox Card

Defeat Check using Stolen or Counterfeit Prox Card

Physical Protection Logic Trees

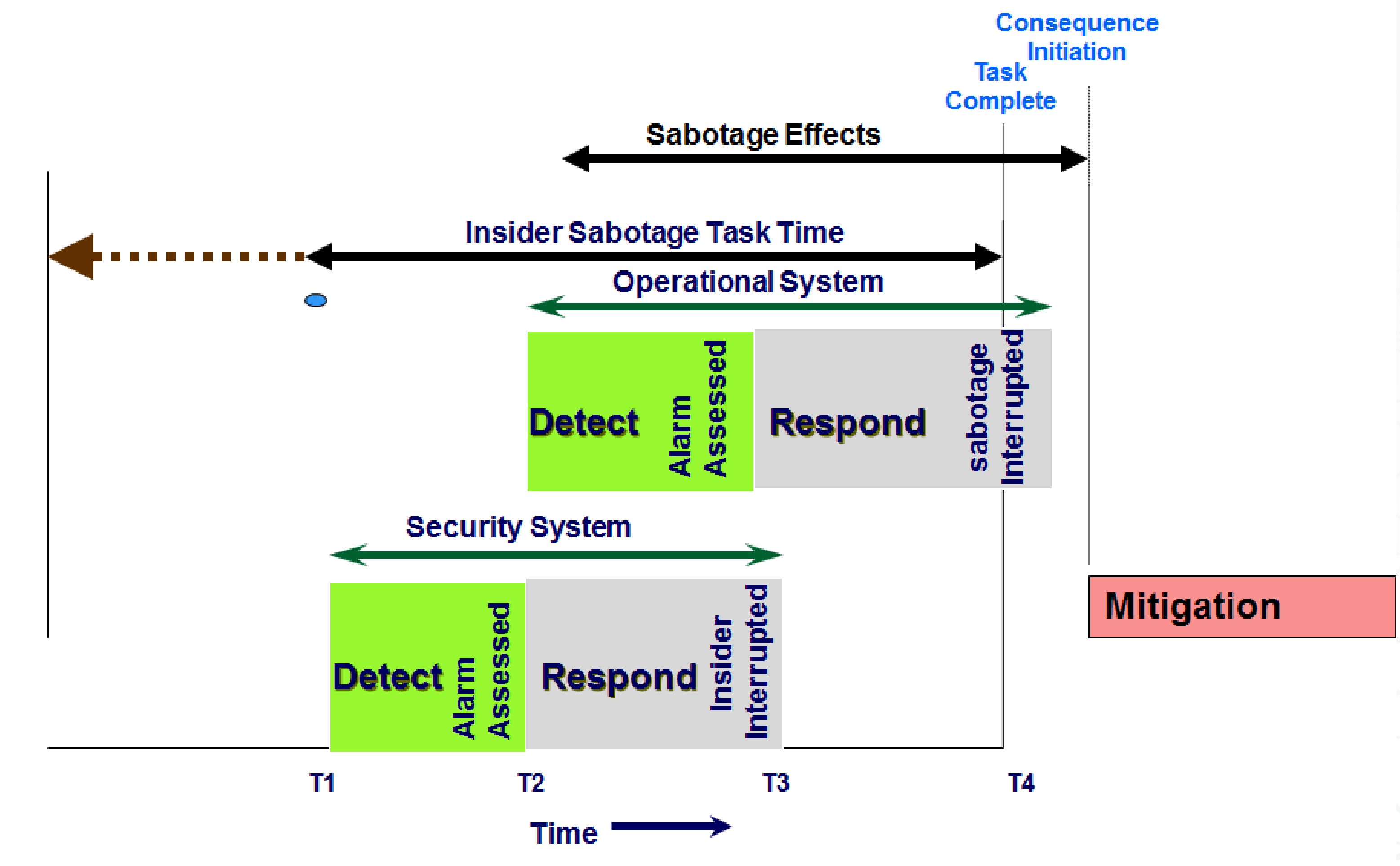
Combine the Results of the Cyber Security Evaluation with the PPS Evaluating

- Uses a modeling framework that successfully models violent insiders colluding with outsiders
- System Effectiveness Metric $P_{E(Total)}$ for scenarios

  $$P_{E(Total)} = 1 - (1-P_{DS})(1-P_{EO})$$

  - P_{DS} is the P_D for the cyber-physical attack during a prolonged stealth preparation for the attack.
  - P_{EO} measures effectiveness of the (degraded) PPS during the attack itself
- Can assign some standard measure, M_C, of the difficulty/cost of the cyber portion of the scenario

Adversary and Response Timelines for Characterizing Insight into $P_{E(Total)}$



Times and probabilities may be ambiguous or indefinite

NRC Cyber Security Regulations and Guidance Documents

- 10 CFR 73.54, Cyber Security Rule
- Guidance documents
  - Regulatory Guide (RG) 5.71 “Cyber Security Programs for Nuclear Facilities” (2010)
  - NEI 08-09 Rev. 6 “Cyber Security Plan For Power Reactors” (2010)
  - NEI 13-10 Rev 2 “Cyber Security Assessments” (2014)

RG 5.71 Conceptual Approach

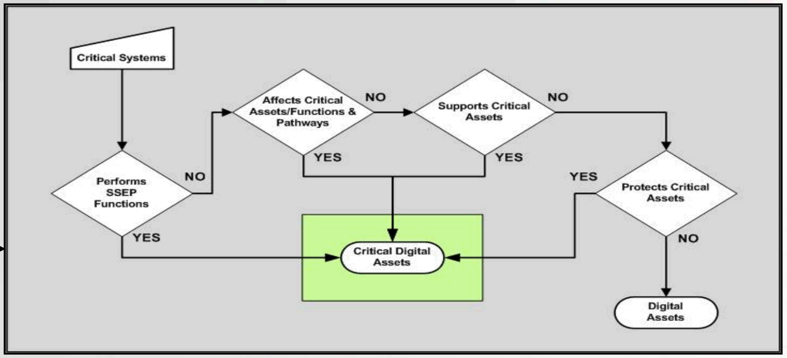
Cyber Security Assessment Team

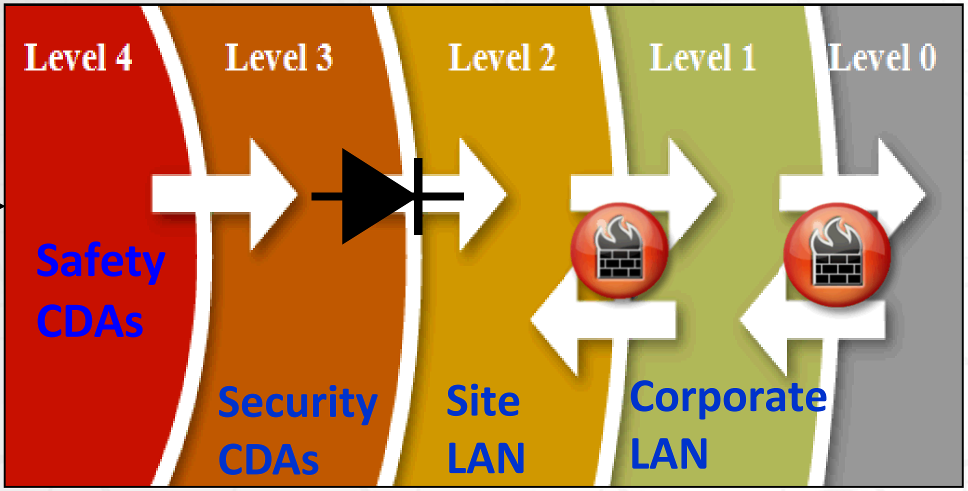
Identify Critical Digital Assets

Apply Defensive Architecture

Address Security Controls

1. Address each control for all CDAs, or
2. Apply alternative measures, or
3. Explain why a control is N/A





Summary and Conclusions

- Described a methodology to evaluate systems against blended cyber-physical attacks on a PPS
- The approach incorporates existing techniques used by cyber security evaluators as well as PPS evaluation techniques
  - Techniques have been shown to be effective over time
  - Training exists for these techniques
- The approach explicitly addresses the interface between the cyber-security evaluation and the PPS evaluation