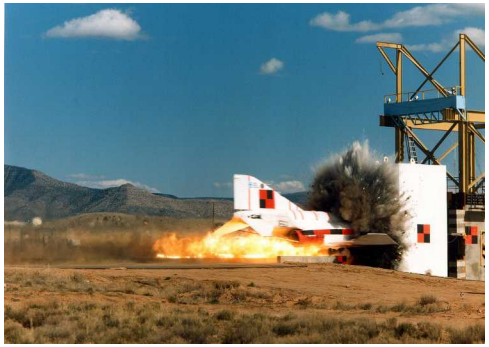
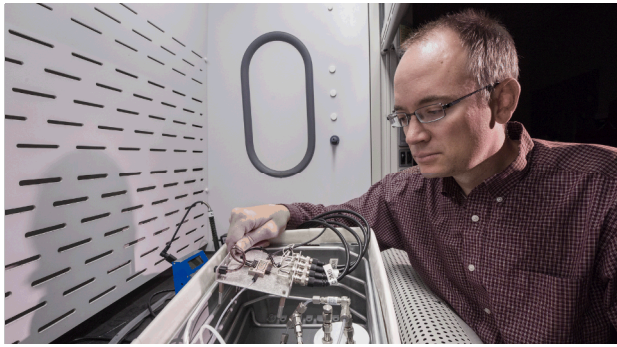
SAND2015-2580C

Exceptional service in the national interest

Sandia National Laboratories





Security Effectiveness Analysis

Overview

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

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. SAND NO. 2011-XXXXP

Evaluation Approaches

- **Expert Opinion**: PPS design and evaluation activities based on personal knowledge and experience
- **Features Approach**: PPS design and evaluation based on specification and implementation of a required set of features (aka *Compliance Approach*)
- **Component Criteria Approach**: PPS design and evaluation based on standards approach that uses performance criteria for *some* security features
- **System Performance Approach**: PPS design and evaluation based on a systems engineering security methodology specifying and achieving an overall system effectiveness against a Design Basis Threat

Evaluation Approaches Summary

Approach	Requirement	Metric
Expert	Satisfy expert	Opinion
Features	Include required features	Presence of features
Component Criteria	Include required features that meet specific standard	Presence of feature and performance standard
System Performance	Prevent theft or sabotage of facility	System effectiveness

Case Study (1 of 4)

- **Situation**: There is an external door on the 28th floor of a high-rise building. The building security officer wants to know if the door needs to be locked.

- **For each of the four approaches**
  - **How do you answer this question?**
  - **How do you validate your answer?**

Case Study (2 of 4)

- **Expert Opinion**: A security expert might tell you that in their opinion it is desirable to lock the door
  - How do you validate that opinion?
  - What if another "expert" gives another opinion? Who is correct?

- **Features Approach**: The company owning the building might require that all external doors below the 20th floor not otherwise identified as entrances for the public or as emergency exits be locked.
  - How would you then determine if the door should be locked?
  - How would you validate that this requirement will lead to better security?

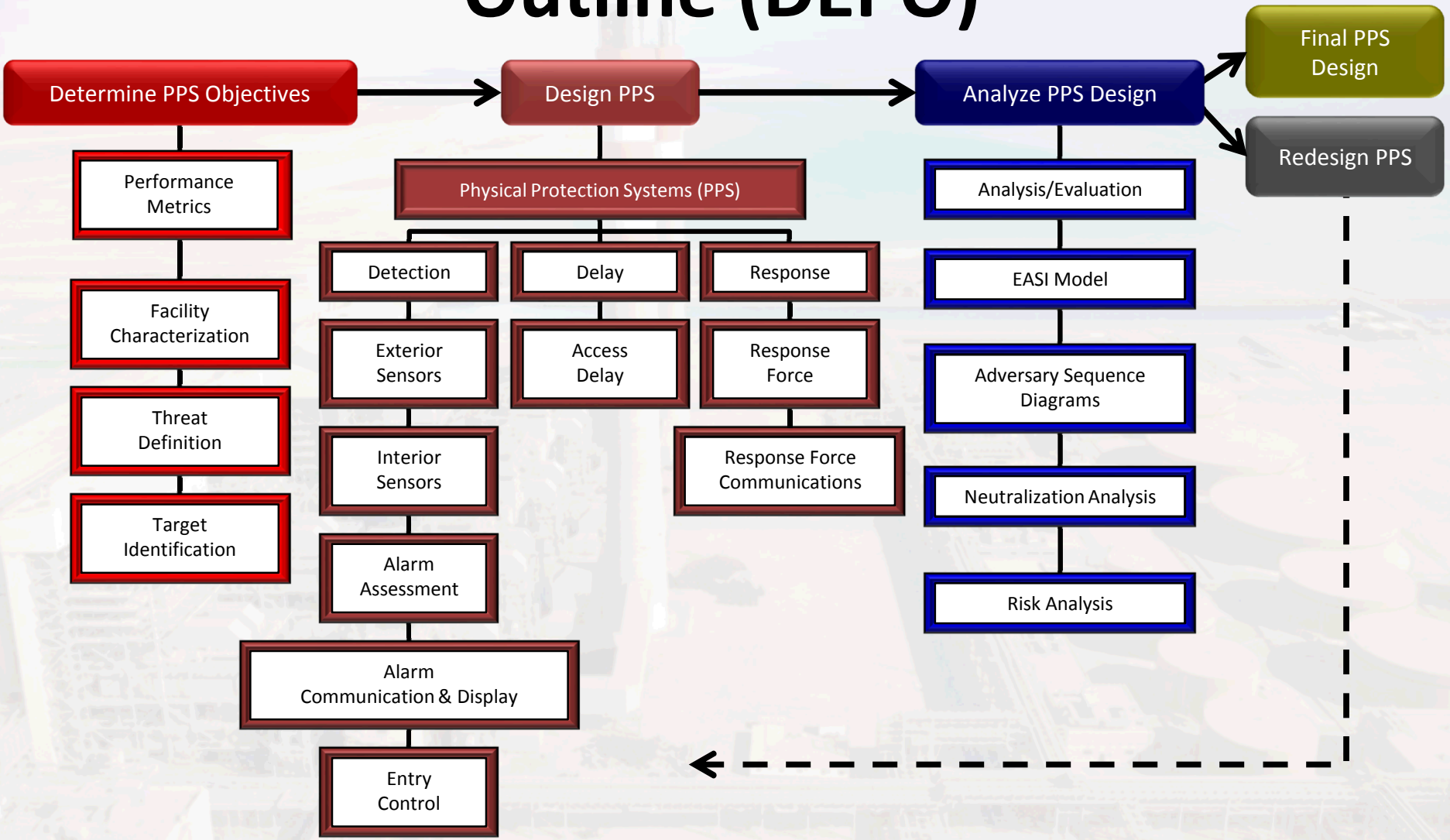
Case Study (3 of 4)

- **Component Criteria Approach**: In this approach, there is a requirement to include required features that meet specific performance standards
  - Example: "all external doors below the 20th floor not otherwise identified as entrances for the public or as emergency exits should be locked and provide at least three minutes of delay against an adversary with a hammer and crow bar."
  - How would you then determine if the door should be locked?
  - How would you validate that meeting this requirement will lead to better security?

Case Study (4 of 4)

- **System Performance Approach**: This approach considers several criteria in a systems engineering methodology
  - Requirements
    - What assets or items in the building need protecting? (*critical targets*)
    - Who do these targets need to be protected from? (*design basis threat*)
    - How well do I need to protect the targets? (*system performance metric*)
    - Are there non-security reasons to lock the door or leave it open? (*facility characterization*)
  - Characterize the Physical Protection System
  - Evaluate the effectiveness of the Physical Performance System
  - How do you answer the "lock or not lock" question?
  - How do you validate your answer with the results of the analysis?

Design and Evaluation Process Outline (DEPO)



Performance Analysis

- **System performance-based process (DEPO)**
- **Metric is acceptable *risk***
  - RC = [1 - (PI * PN)] * C
  - PI = Probability system will interrupt
    (*detection, assessment, delay, response time*)
  - PN = Probability response force will neutralize
    (*response force vs. adversary*)
  - C = Consequence of a successful attack on a target
    (*impact on SYSTEM*)

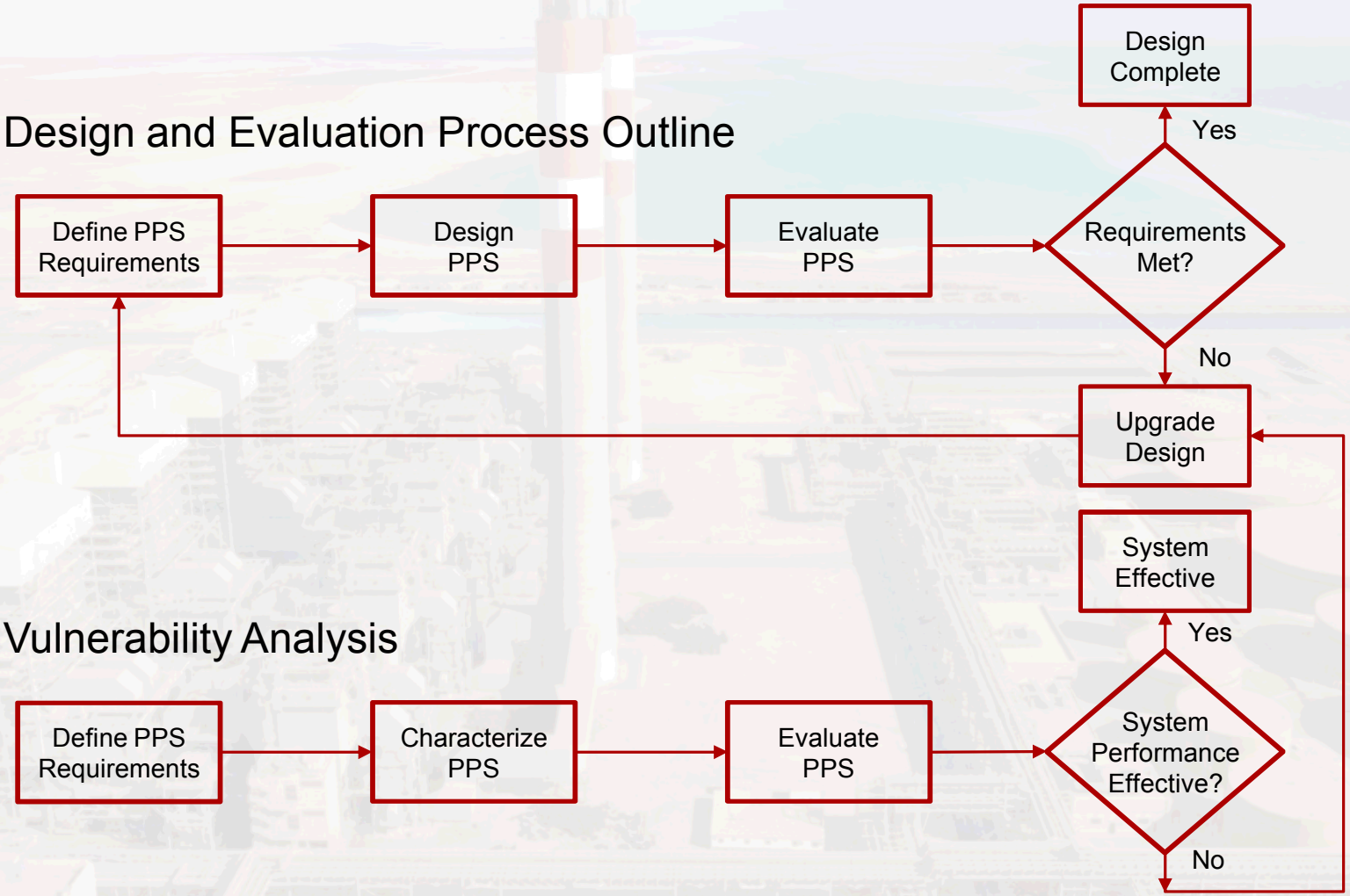
Primary PPS Functions

- **Detection** – the discovery of an adversary action
  - Accomplished with alarms generated by sensors
  - Alarms must be reported and assessed

- **Delay** – the slowing down of adversary progress after detection
  - Accomplished with barriers, personnel, locks, active and passive delay technologies

- **Response** – the actions taken by response forces to prevent adversary success
  - Response force deployment
  - Tactics, techniques, and procedures
  - Equipment

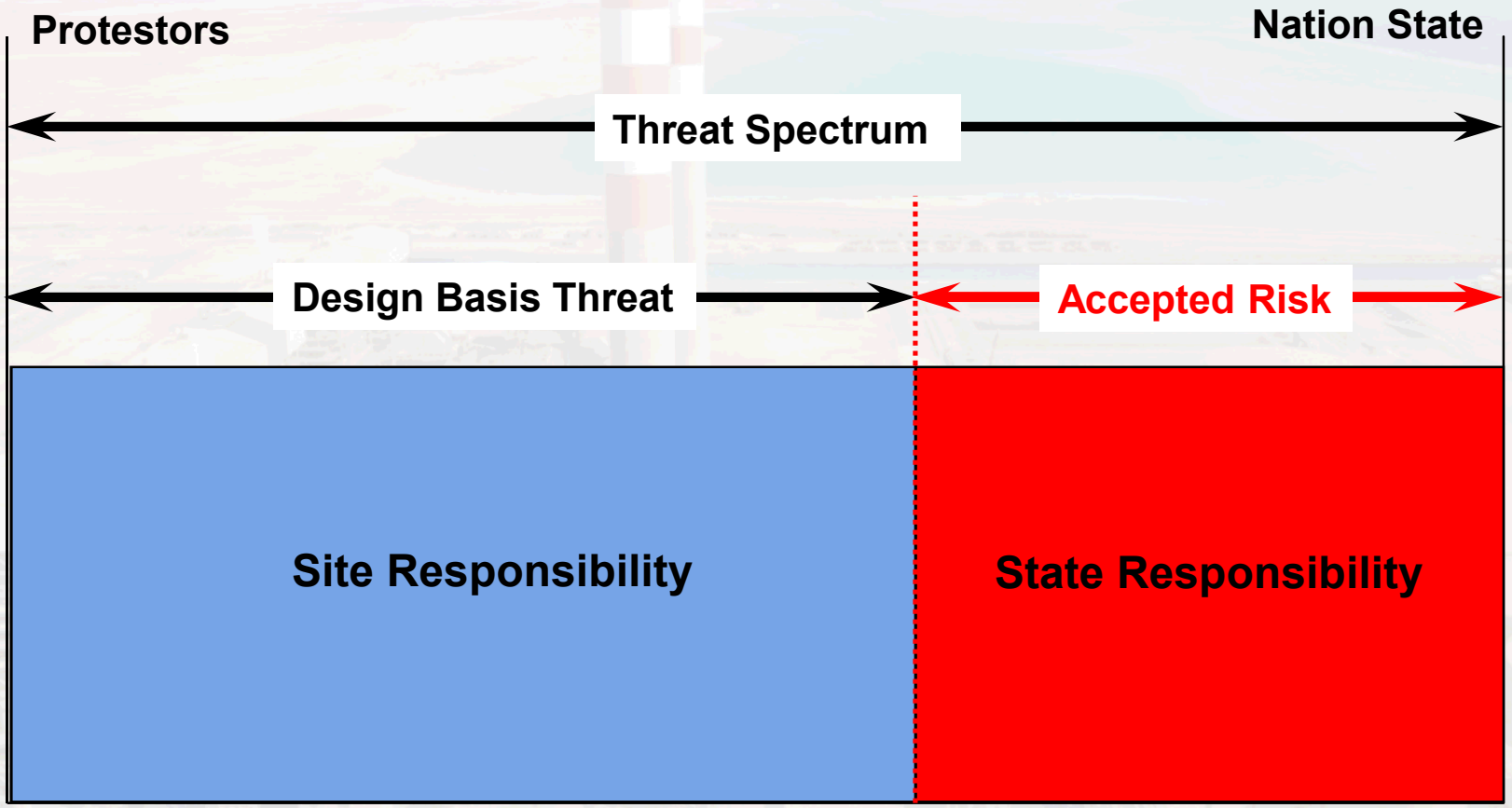
DEPO vs. VA


Design and Evaluation Process Outline
Define PPS Requirements
Design PPS
Evaluate PPS
Requirements Met?
Yes
No
Design Complete
Upgrade Design
Vulnerability Analysis
Define PPS Requirements
Characterize PPS
Evaluate PPS
System Performance Effective?
Yes
No
System Effective

Threat Analysis

- **National level effort**
- **Examine entire threat spectrum**
  - Protestors
  - Criminals
  - Terrorists
- **Sources of information**
  - Intelligence
  - Police
  - Historical data
- **Demonstrated and emerging capabilities**
- **State, regional, international threats**

Design Basis Threat



DBT Example

Motivation	Ideological, political
Intent	Sabotage
Numbers	8 with multiple teams – based on capabilities and trends
Weapons	RPG, grenades, small arms, standoff and IDF
Explosives	Mix of commercial, military (C-4) and homemade; VBIED; shaped charges
Tools	Hand tools, power tools, electronics, night vision, stolen items
Transport	Ground, sea, maritime, air (helicopter)
Tech skills	Paramilitary training, explosives, engineering, IT
Funding	Mid to high level – regional support
Support structure	Local cell structure, safe-havens, sympathetic population
Insider Collusion	1 – 2: passive and/or active, non-violent insider (active/violent???)

Facility Characterization

- Physical conditions
  - Site boundaries
  - Weather extremes and effects on operations
  - Terrain analysis
    - Key Terrain – choke points, corridors, observation platforms
    - Observation/Fields of Fire – areas of cleared vegetation, fields
    - Cover and Concealment – ballistic vs. non ballistic, trees, culverts
    - Obstacles – drainage, adjoining buildings, terrain, HVAC, pipes
    - Avenues of Approach – various types of roads, paths (by size)
- Facility operations (day vs. night)
  - Products and processes
  - Operational hours
  - Numbers of employees

Facility Characterization

- Facility policies and procedures
  - Operational policies
  - Training policies
  - Corporate culture
- Regulatory requirements
  - Federal, state, local
  - Regulatory authority
- Safety requirements
  - Safety regulations and requirements
  - Security regulations and requirements
  - Interaction between safety and security

Facility Characterization

- Legal issues
  - Liability for event
  - Failure to protect
  - Overreaction by security forces
- Corporate goals and objectives
  - Management's view of security
  - Level of support for security initiatives
  - Security Culture

Target Examples

- People (employees, families)
- Transmission lines
- Towers
- HV Transformers
  - System controls
  - Cooling oil
  - Radiator
  - Coils
- System distribution – multiple axis attack on nodes

Targets and Consequences

- Examine site performance as ***system***
  - Important high value targets *may not affect* overall system
  - Identify key nodes (offsite?)
  - Analyze repair and replacement times
  - Analyze possible damage mechanisms
- Assign consequence value based on impact
- Determine performance level of PPS

$$R_C = [1 - (P_I * P_N)] * C$$

(0.2) (0.9)

(0.78)

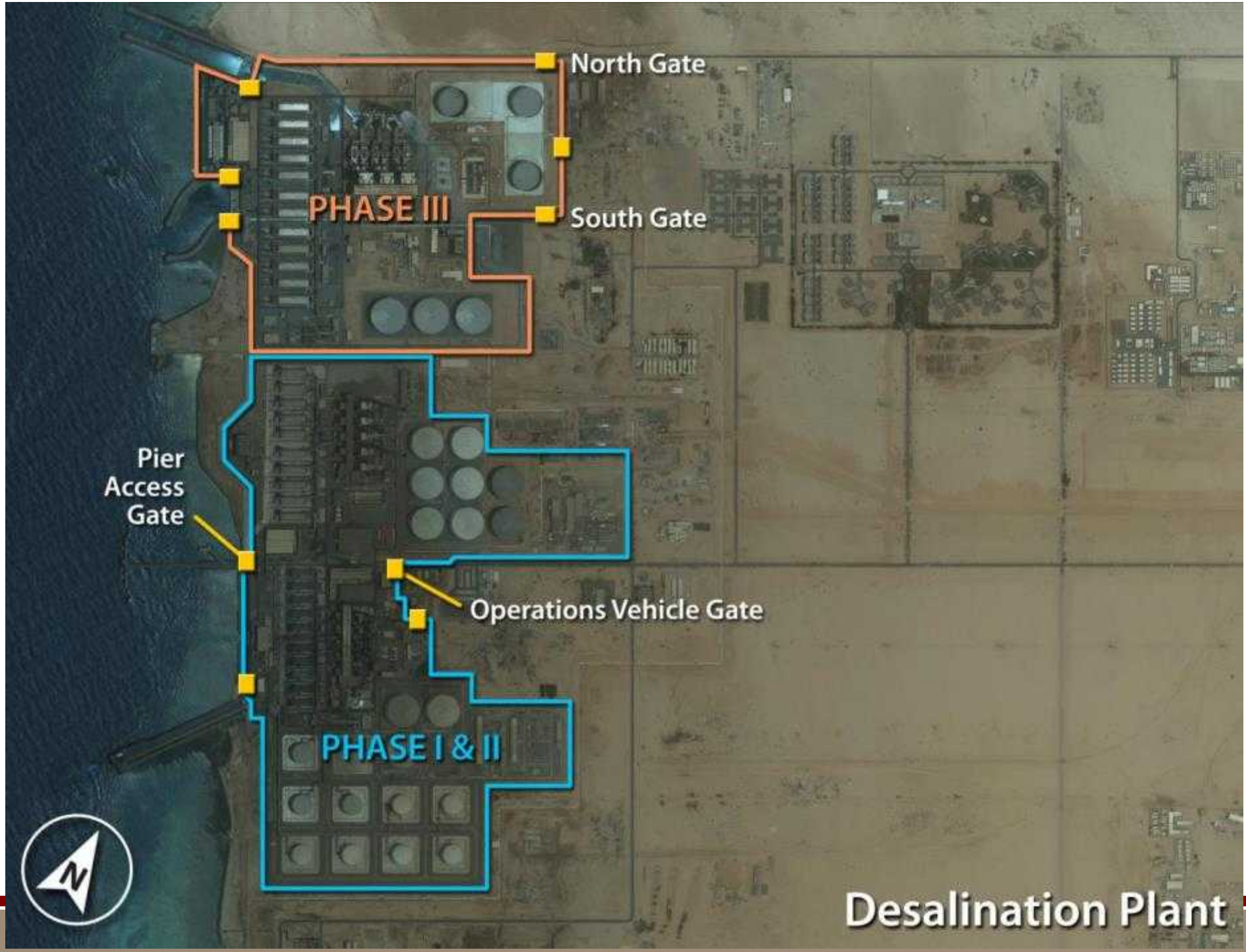
Targets and Consequences

- As acceptable risk is reduced, P_E must increase

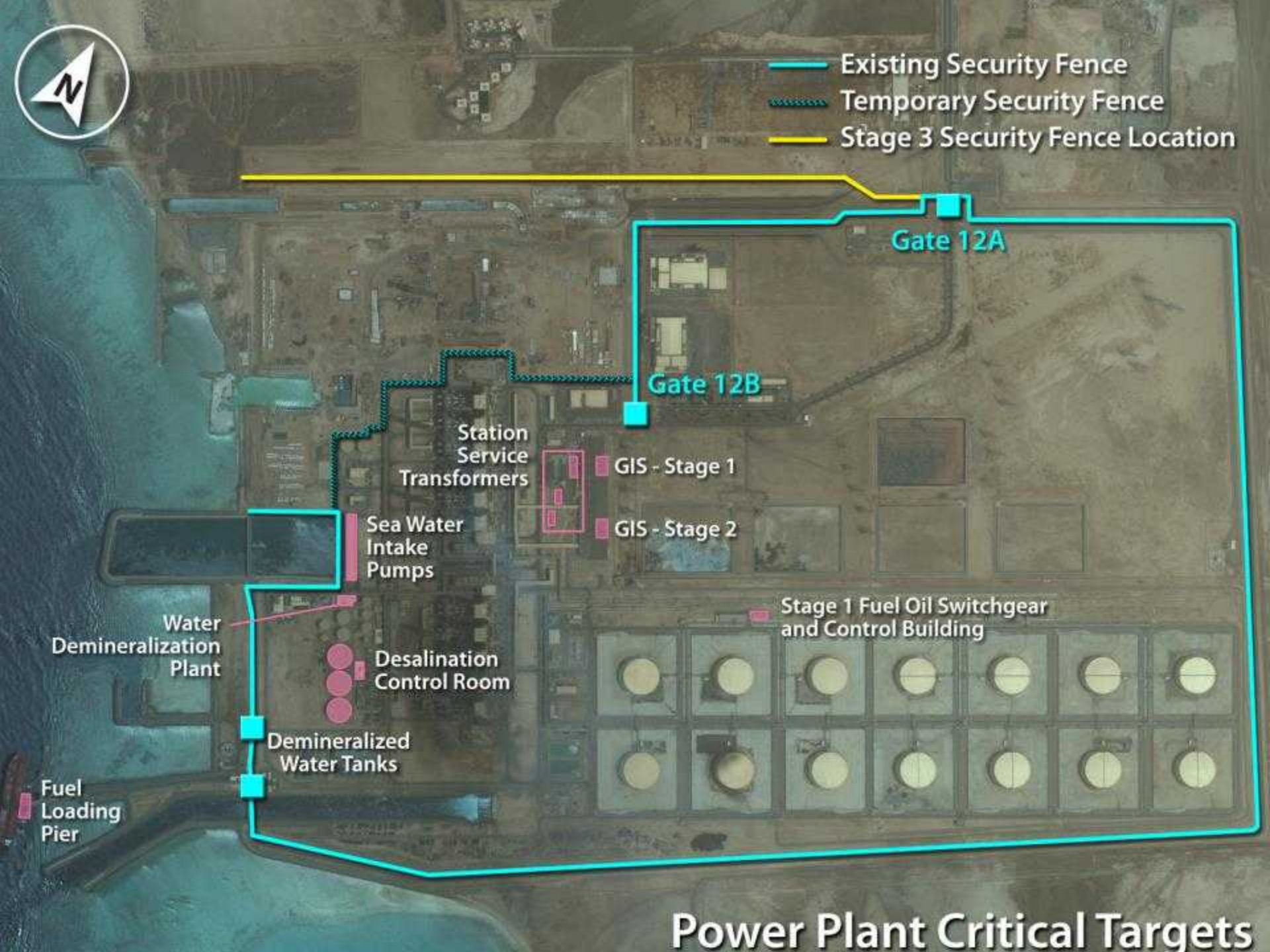
$$R_C = [1 - (P_I * P_N)] * C$$

(0.05) (0.9)

(0.94)


North Gate
PHASE III
South Gate
Pier
Access
Gate
Operations Vehicle Gate
PHASE I & II
N
Desalination Plant


Turbine Hall
Gas Insulated Switchgear
Auxiliary Tranformers
Sea Water Intake Switchgear
Gas Insulated Switchgear
Pump Station Transformer
Sea Water Pump Station
Gas Insulated Switchgear
Sea Water Pump Station
N
Critical Targets


Existing Security Fence
Temporary Security Fence
Stage 3 Security Fence Location
Gate 12A
Gate 12B
Station Service Transformers
GIS - Stage 1
GIS - Stage 2
Sea Water Intake Pumps
Water Demineralization Plant
Desalination Control Room
Stage 1 Fuel Oil Switchgear and Control Building
Demineralized Water Tanks
Fuel Loading Pier
Power Plant Critical Targets

Characterize the PPS:

- Characterize protection elements in depth
  - Detection, Delay, Response
- Include access controls and procedures
- Develop methods for defeating the protection system elements
- Evaluate metrics for detection and delay
- Characterize the response in terms of capabilities and Response Force Times (RFTs)

The output will be a thorough description of the PPS for all significant targets

Types of Exterior Sensors

- Fence Disturbance
- Taut Wire Fence
- Electric Field or capacitance sensors
- Active infrared
- Passive infrared
- Bistatic and monostatic microwave
- Dual technology sensors
- Video motion detection
- Area denial – RADAR
- Ballistic/sniper detection - Boomerang

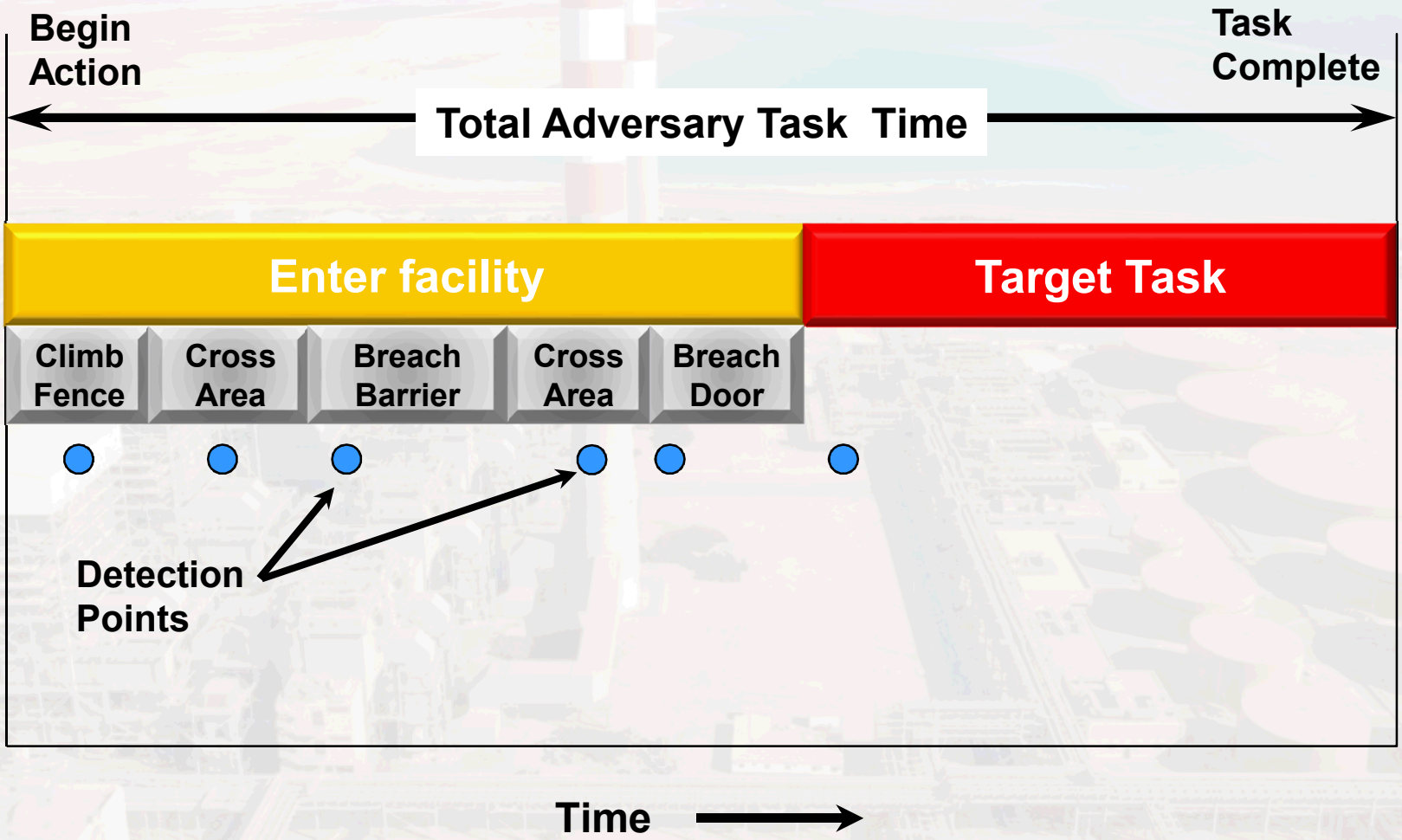
Sensor Selection Considerations

- Application
- Operating principle
- Detection capabilities
- Conditions for unreliable detections
- Typical defeat methods
- Major causes of nuisance alarms

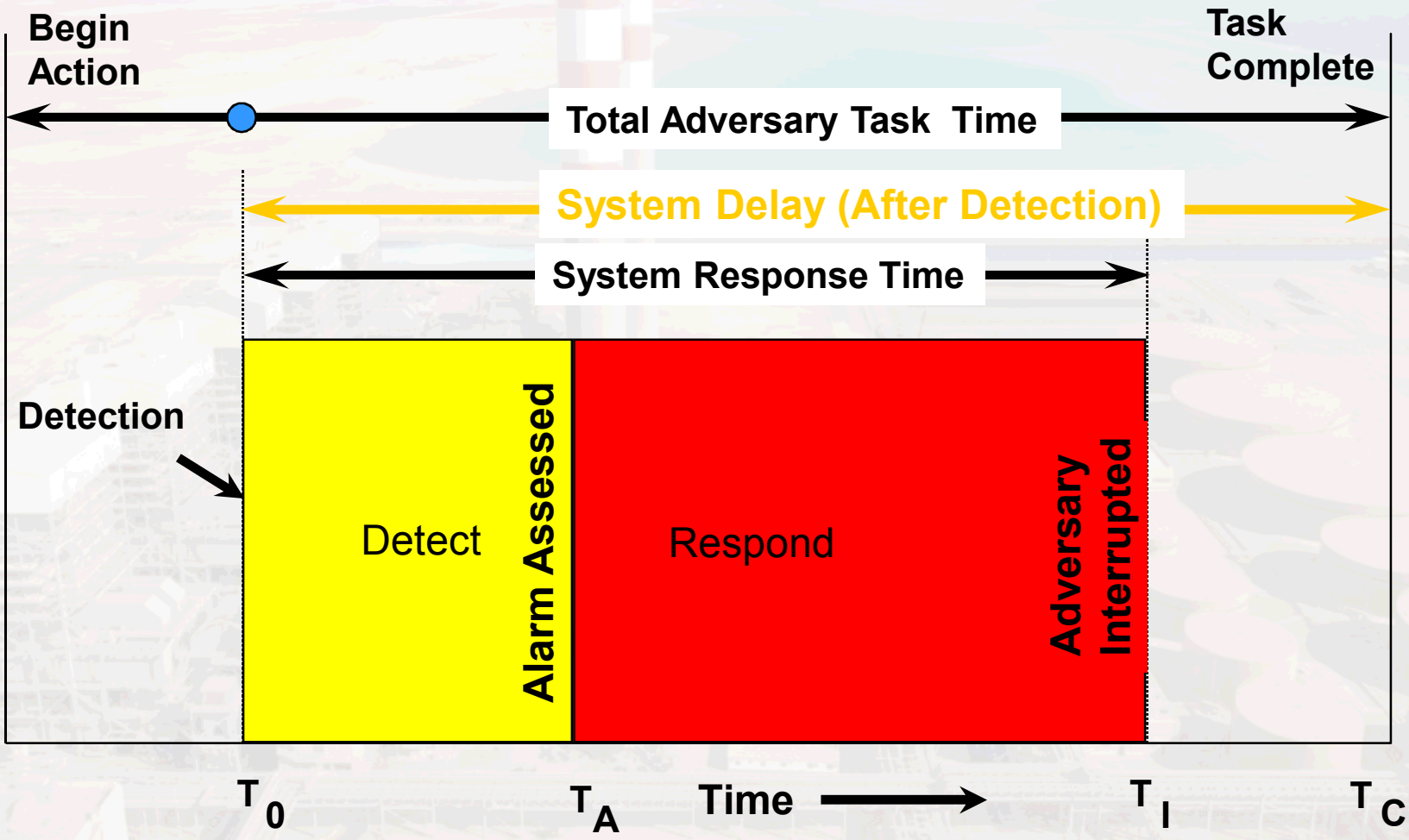
Adversary Path Concept

- Adversary must *traverse a path* from offsite to the target
- Path is composed of a *series of actions*
- Each action has a *delay time* based on DBT capabilities
- *Detection* may occur at various points along the path
- Detection may be minimized or defeated based on DBT capabilities
- Response Force may *interrupt* the adversary if detection is timely

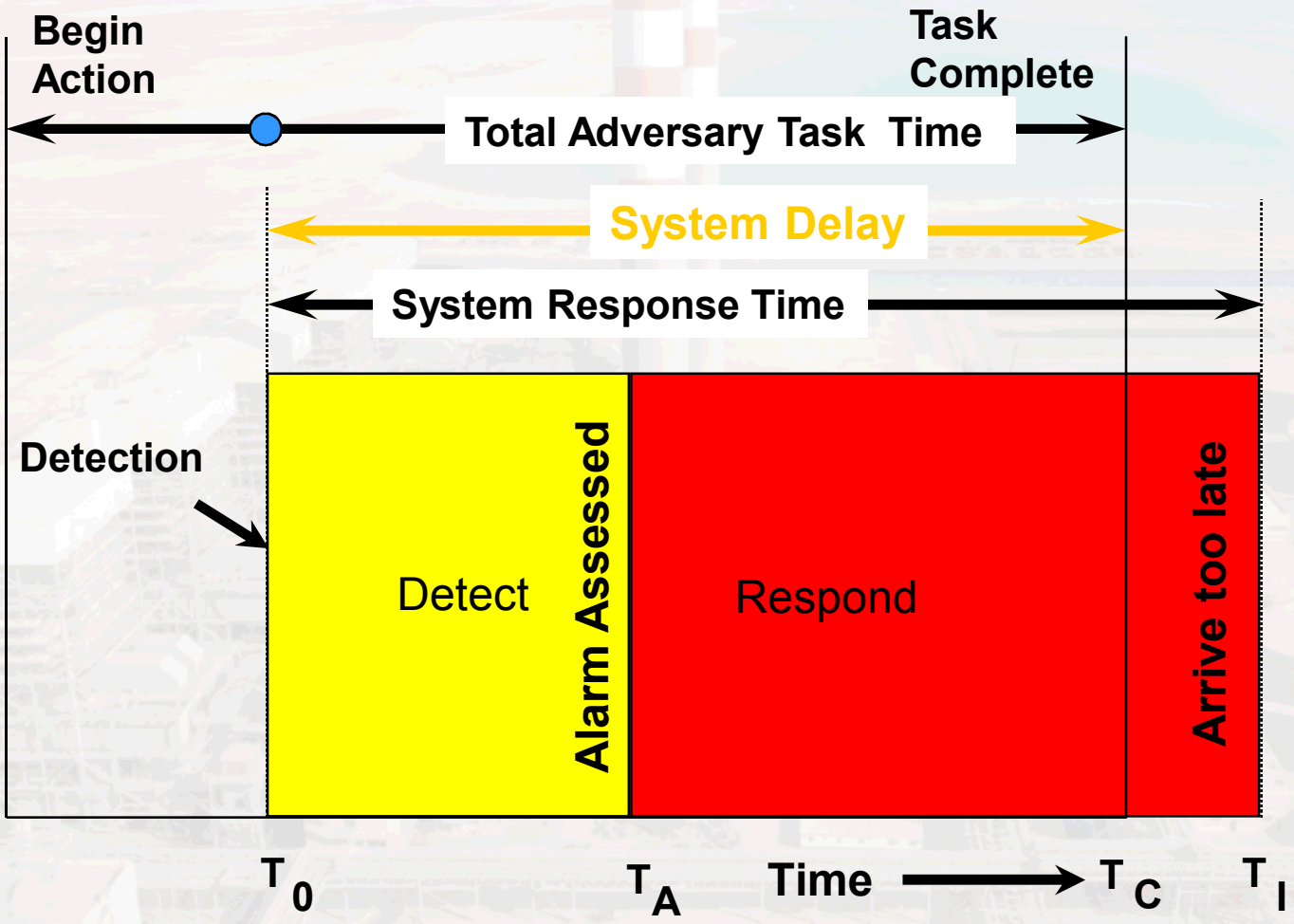
Example of Adversary Path



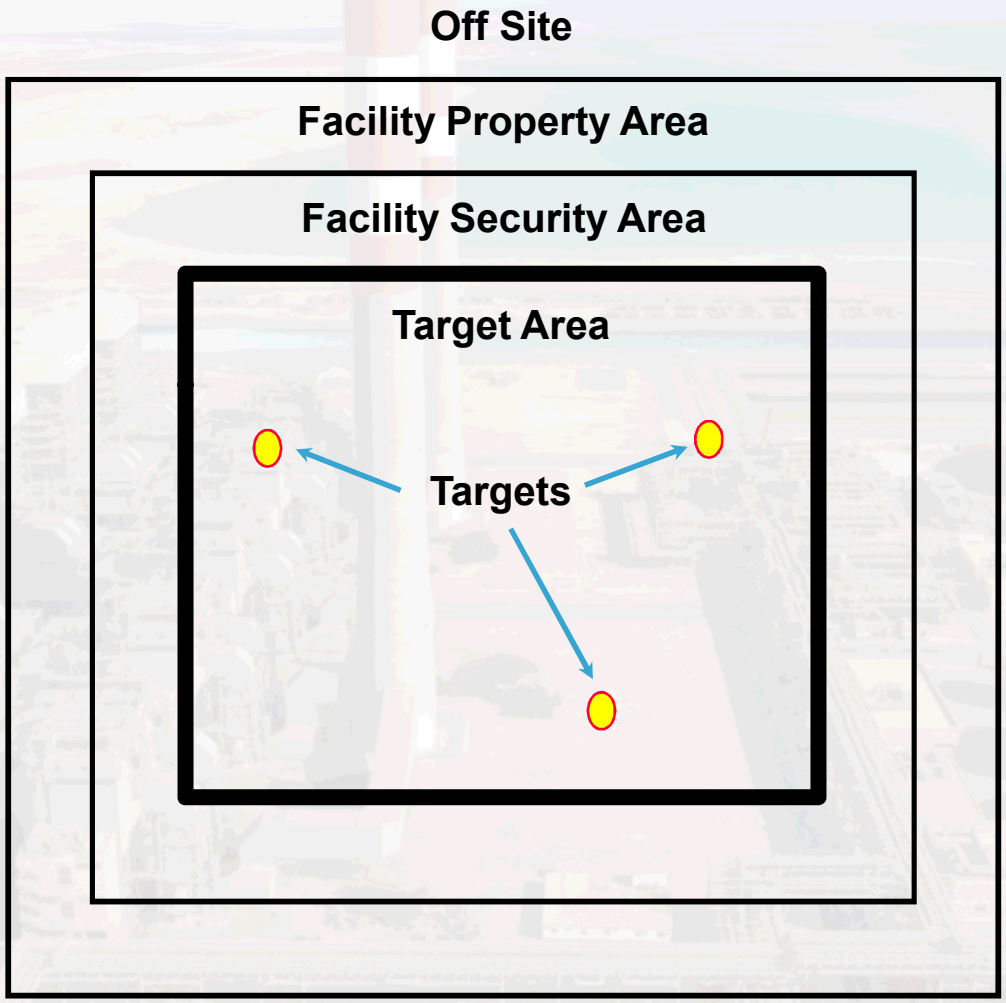
Example of Timely Detection



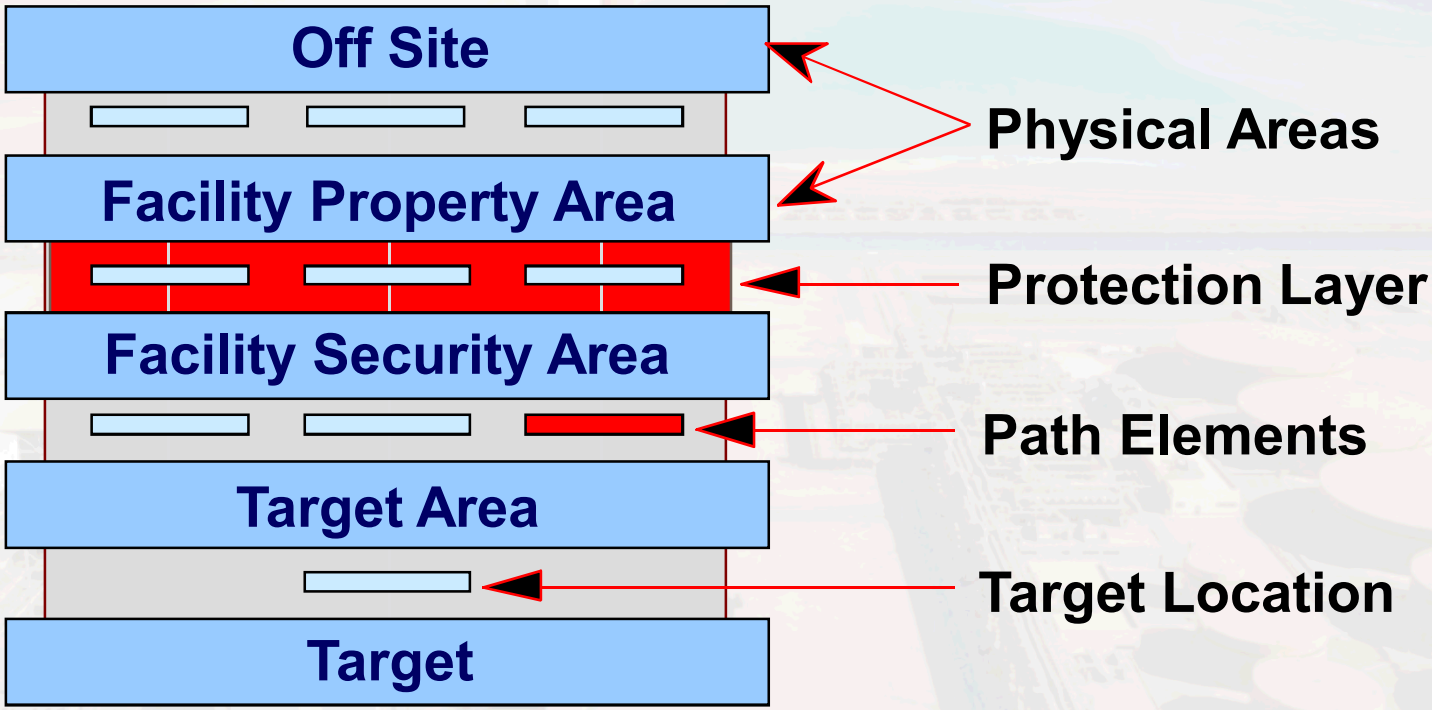
Example of Non-Timely Detection



Facility Model



Adversary Sequence Diagram



Performance Test Demonstration

- Barrier Defeat Techniques
  - Unassisted fence climb – dual penetration
  - Assisted fence climb
  - Climb under fence
  - Use of outside debris/structures to assist
- Sensor Defeat Techniques
  - Jump
  - Crawl

Physical Security Best Practices

- Protect pencils like pencils; diamonds like diamonds
- Protection in depth
- Balanced protection
- Multiple complimentary sensors
- Delay (barriers) *after* detection and assessment
- Response force inside protective perimeter
- Defend and deny key targets
- Mass and firepower