SAND2024-1056C

ADVANCED REACTOR SAFEGUARDS & SECURITY

Cyber Integration, Remote and Autonomous Operations

Cyber-Physical Blended Attacks

PRESENTED BY

Pat Moosir

5/14/24

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

Outline

Assumptions

Objective

Background

- Physical Protection Systems (PPS) approaches for Advanced Reactors
- Styles of Cyber Attacks

Work Completed

- Cyber security associated with PPS

Looking to the rest of the FY

- Coordination with ARSS cyber-security projects

Conclusions

Assumptions on the Reactor site

A facility is using the current rulemaking to license their reactor site, e.g. 10CFR73 in combination with 10CFR50/52

The physical protection system (PPS) is completely wired with no wireless communication between any of the components

- Meaning a cyber attack on your PPS sensors has to occur on-site

A perimeter intrusion detection and assessment system (PIDAS) is incorporated into the PPS design

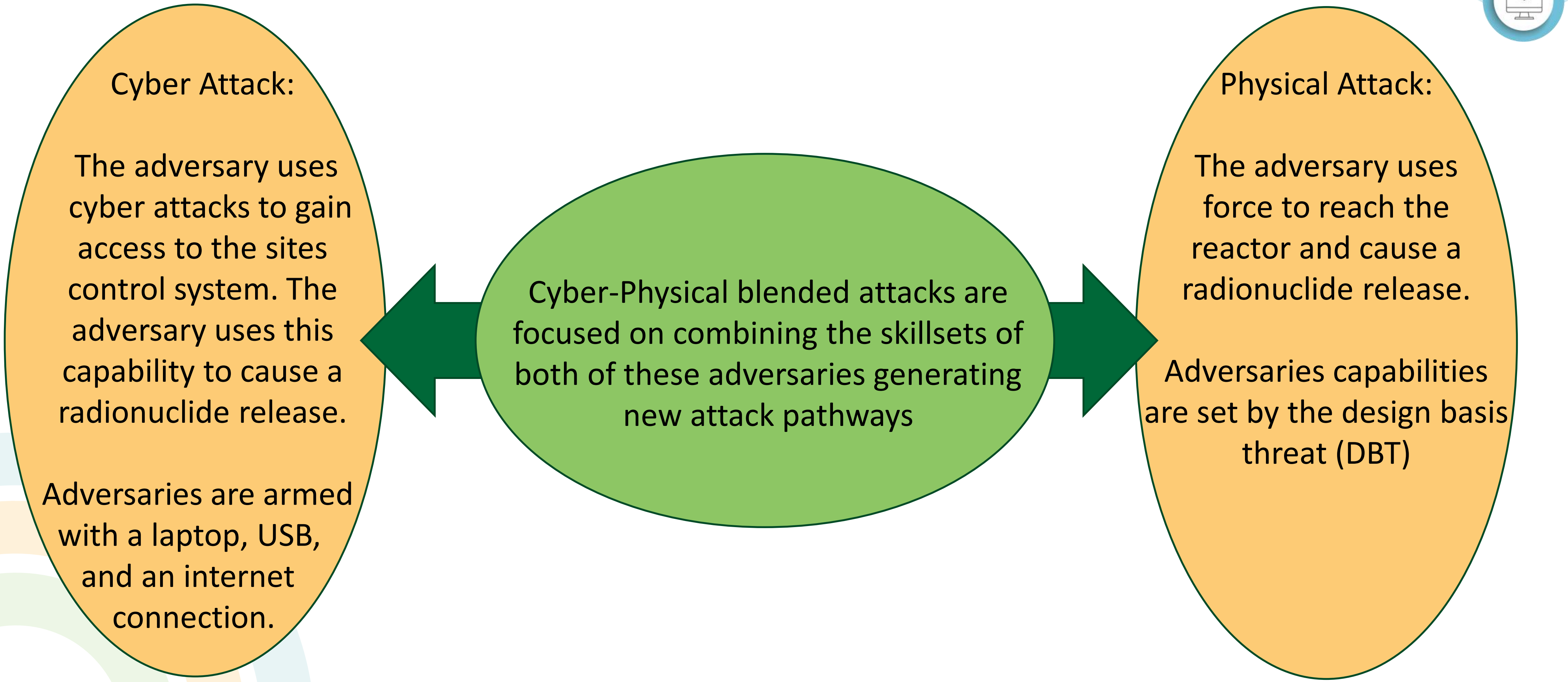
- Microwave sensors
- Vibration sensors
- Closed-Circuit Cameras

Objective

- Cyber-physical blended attacks, potentially, open up reactors to new attack pathways requiring reactor vendors to look into the cyber security approaches required as reactors move to autonomous monitoring and control

Not a new thing, just a new focus

Cyber-Physical Blended Attacks



Cyber Attack:

The adversary uses cyber attacks to gain access to the sites control system. The adversary uses this capability to cause a radionuclide release.

Adversaries are armed with a laptop, USB, and an internet connection.

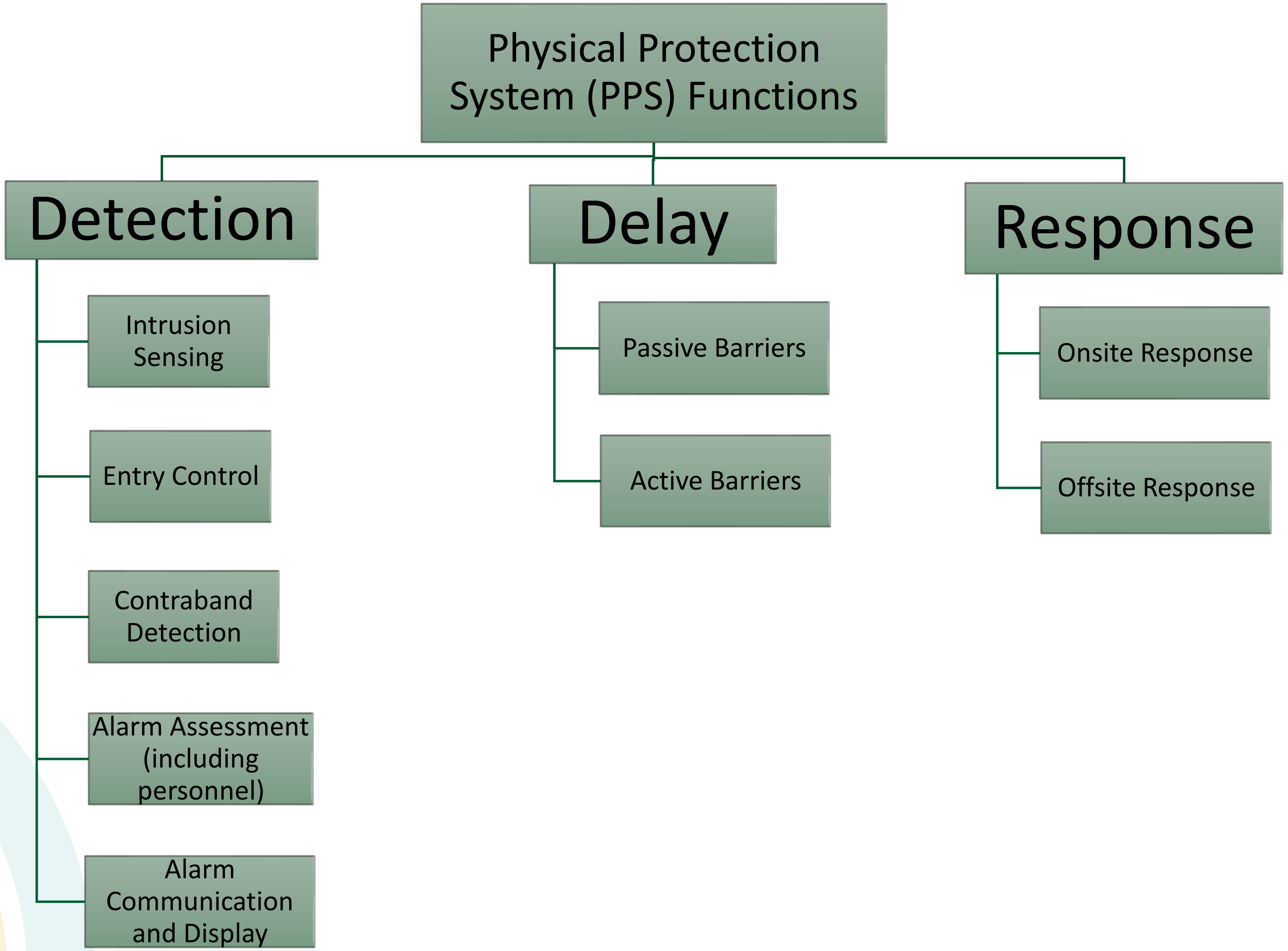
Cyber-Physical blended attacks are focused on combining the skillsets of both of these adversaries generating new attack pathways

Physical Attack:

The adversary uses force to reach the reactor and cause a radionuclide release.

Adversaries capabilities are set by the design basis threat (DBT)

PPS Philosophy: Detection, Delay, Response



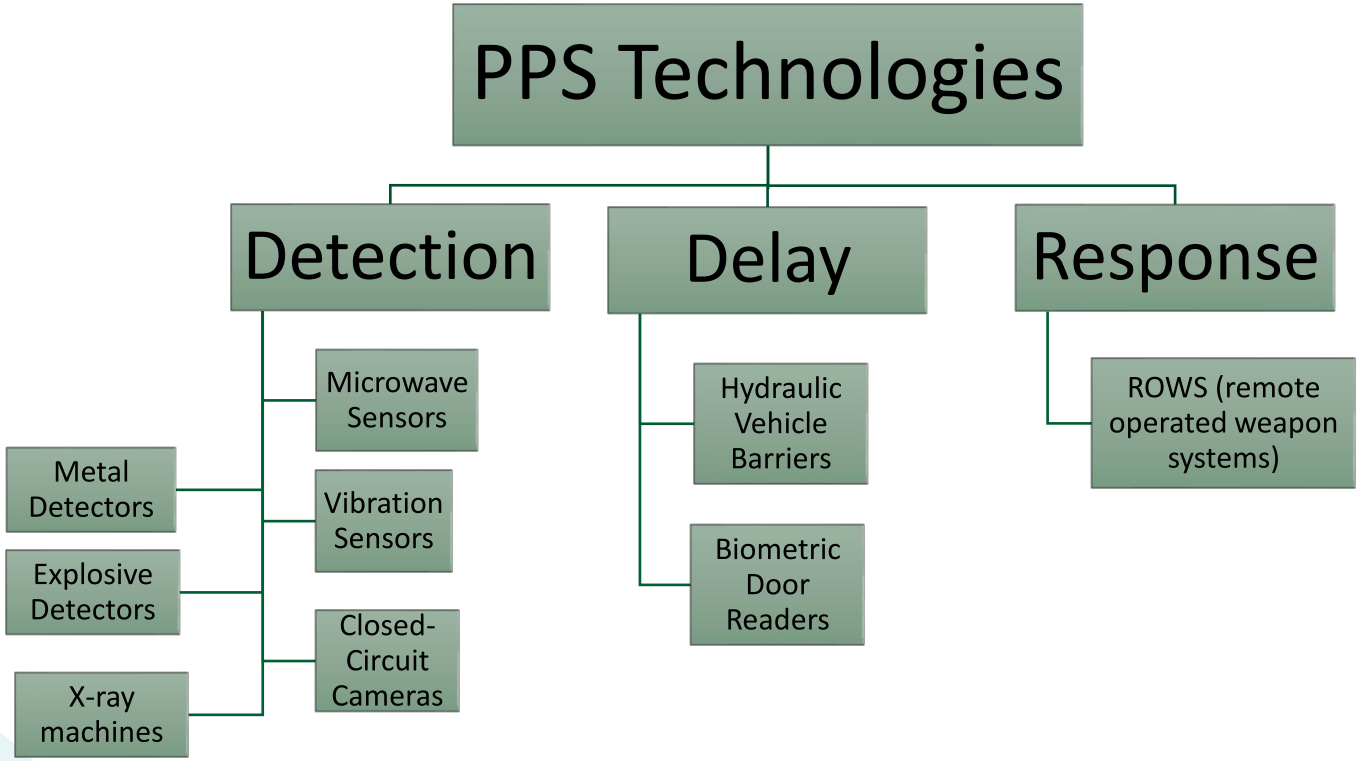
Physical Protection System (PPS) Functions

Detection
- Intrusion Sensing
- Entry Control
- Contraband Detection
- Alarm Assessment (including personnel)
- Alarm Communication and Display

Delay
- Passive Barriers
- Active Barriers

Response
- Onsite Response
- Offsite Response

PPS Technologies Associated with Detection, Delay, and Response



- PPS Technologies
  - Detection
    - Microwave Sensors
    - Metal Detectors
    - Vibration Sensors
    - Explosive Detectors
    - Closed-Circuit Cameras
    - X-ray machines
  - Delay
    - Hydraulic Vehicle Barriers
    - Biometric Door Readers
  - Response
    - ROWS (remote operated weapon systems)

Different styles of blended-cyber attacks

Attack Class	Description	Attack Goals
Reconnaissance	Adversary is trying to gather information they can use to plan future operations	These styles of cyber-attacks may begin very early in the attack timeline, e.g. the planning period. Attacks on DNS (internet phonebook), email phishing, email addresses, employee information, credential identification are all possible with these styles of attacks
Resource Development	Adversary is trying to establish resources they can use to support operations	
Initial Access	Adversary is trying to get into your network	

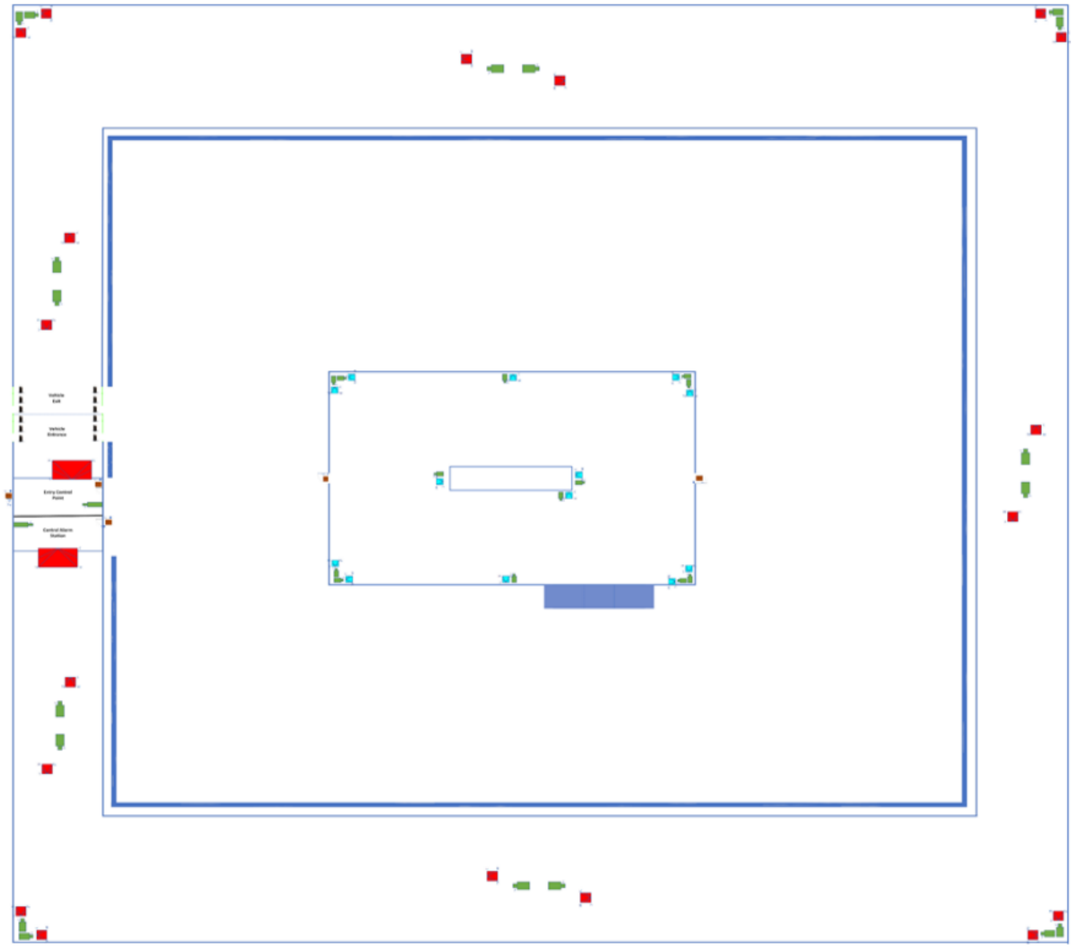
I will not discuss each attack class associated with cyber, but outline a few with similar goals that will impact PPS

More information can be found at https://attack.mitre.org

Different styles of blended-cyber attacks

Attack Class	Description	Attack Goals
Initial Access	Adversary is trying to get access into your network	These styles of cyber-attacks directly impact the PPS's performance and depending on the PPS may need to occur on-site or prior to the attack These attacks, if successful, allow the adversary to circumvent PPS technologies and introduce new attack pathways
Execution	Adversary is trying to run malicious code	
Persistence	Adversary is trying to maintain their foothold	
Credential Access	Adversary is trying to steal account names and passwords	
Impact	Adversary is trying to manipulate, interrupt, or destroy your systems and data	

PIDAS Layout



Scribe3D Modeling of Microreactor Site

Scribe is used to visualize the PPS sensors and equipment

Equipment within the fences is visualized and the wired connections are tracked to specific field distribution boxes (FDB)

Equipment within the buildings: sensors, biometric door readers, and cameras.

Cyber-attacks investigated

2 classes of blended attacks have been investigated:

Cyber attacks focused on gaining information of the reactor site.

- Assumes adversary gained access to emails sent outside of the site and uses that information to optimally plan their attack.

During the physical attack, the adversary performs a cyber attack with a USB with malware.

- Assumes adversary’s cyber attack completely takes out all equipment associated with the PPS.

Sensor loss impact on attack

- Losing different sensors had more or less impact on the attack.
- Components associated with detection had the least impact on the attack, with delay and response having bigger effects

Minimal Impact	Moderate Impact	Severe Impact
Biometric Door Sensors, Microwave Sensors, Vibration Sensors	Cameras	Hydraulic Vehicle Barriers, ROWs

Lessons Learned

- Implementing blended attacks shows the importance of response in the PPS design philosophy.
- The importance of security by design should incorporate delay components like ankle-breakers or shark cages.
- If any singular component is needed for your system, a cyber attack could make your PPS completely useless.

Unity Engine + ARCADE

- Advanced Reactor Cyber Analysis and Development Environment (ARCADE) is a software simulates cyber attacks and show how the programmable logic controllers (PLCs) are impacted and impact the entire system
- A Unity engine, modeling a AR, has been connected to ARCADE with work remaining in FY24 visualizing cyber attacks on ARs

DCSA for a PPS

- Defensive Cyber-Security Architecture (DCSA) is being combined with this project to develop DCSA for PPS
- DCSA would develop “zones” to protect the more important PPS components
- This work will have primary results this FY

Conclusions

- Cyber-physical blended attacks allow new pathways and show the importance of a strong cyber-security culture at reactor sites
- The impact of cyber attack on specific components impact falls similar to the PPS design philosophy: Detect, Delay, and Response
- Work has begun this FY integrated with ARCADE and DCSA
  - ARCADE has integrated with a Unity engine
  - DCSA integration will begin in the coming months

Thank you for your time and attention!

Contact Information

Pat Moosir mhiggin@sandia.gov