ADVANCED REACTOR SAFEGUARDS & SECURITY

Cyber-Physical Attack

PRESENTED BY

Andrew S. Hahn

April 29th 2026

SAND2026-20442PE

Cyber-Physical Tabletop Purpose

- Combine cyber and physical attacks are an emerging threat which is not well understood.
- Cyber-physical tabletop exercises provide insight to how such coordinated attacks precipitate.
- Physical tabletops are mature practices
  - Scribe3D provides the physical security tabletop platform.
- Cyber tabletops are novel and evolving
- Understanding how cyber attacks change the effectiveness of the physical security is key to protecting facilities from blended attacks.

Cyber-Physical Tabletop

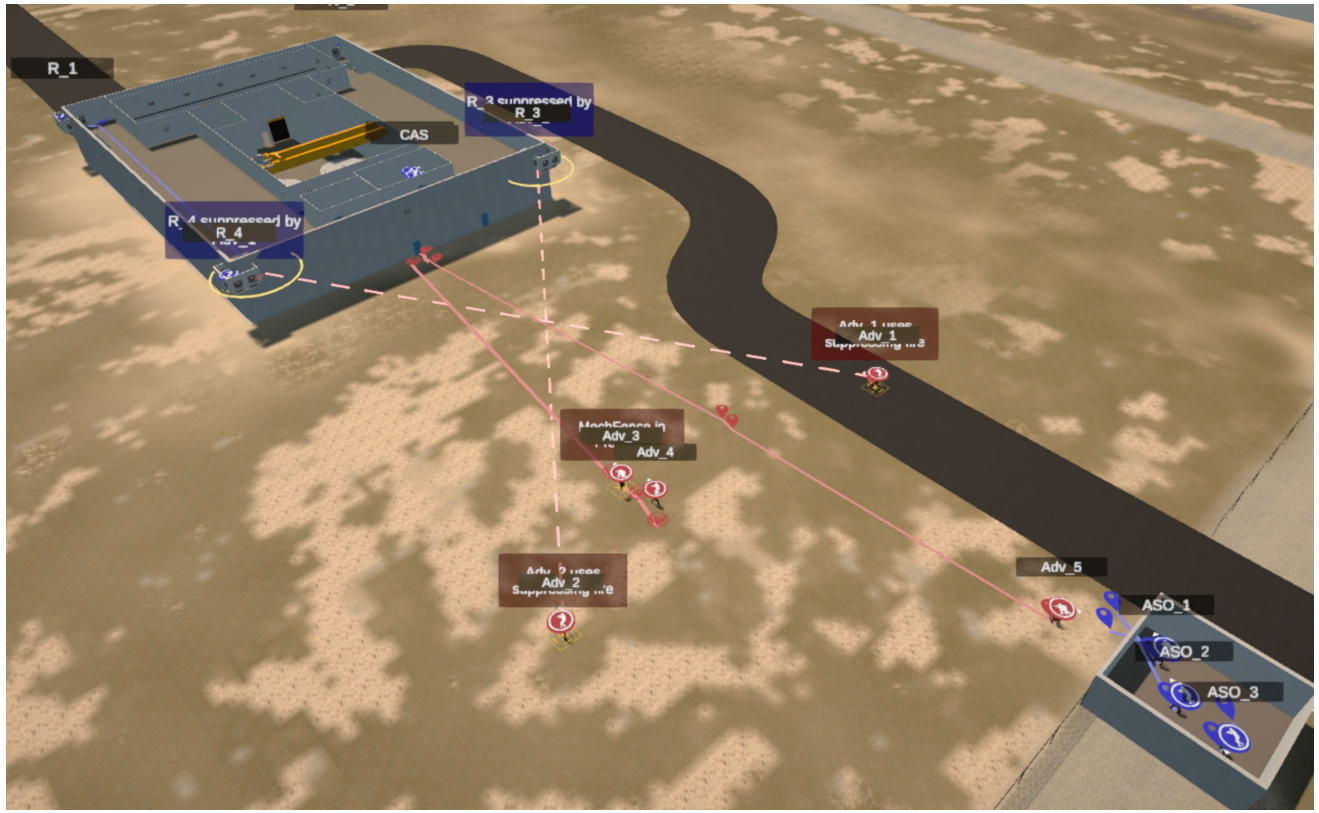
- An integrated team of cyber and physical security SMEs executed a streamlined series of cyber-physical scenarios against advanced reactor designs.
- 3 facility designs were tested
  - An SMR facility designed by Sandia to be inherently defensive
  - A micro reactor facility designed by Sandia with security-by-design features
  - An iPWR facility based on conventional security principals
- Cyber attacks were set as precursors to the physical attacks
  - These cyber attacks were reduced to their effects on the performance of the physical protection system (PPS)

Cyber-Physical Tabletop (Cont.)

- The cyber attacks consisted of degrading the effectiveness of 3 critical PPS functions:
  - Camera's ability to detect the adversary
  - Badged door locks not providing delay
  - PIDAS losing detection ability
- These three effects were then evaluated in all combinations
  - Cameras + Badges, Cameras + PIDAS, Badges + PIDAS, Cameras + Badges + PIDAS
- The effects of cyber attack were the focus as the likelihood of attack and attack success can't be quantitatively assessed.

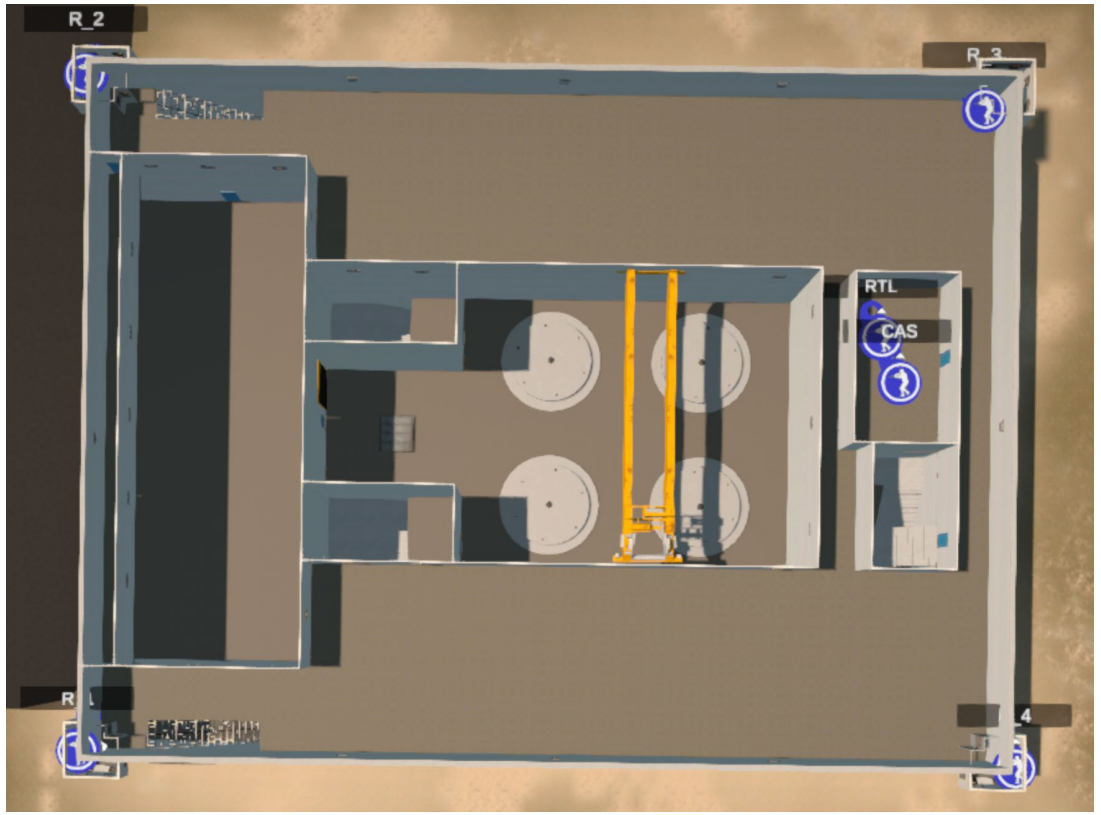
iPWR Facility – Mezzanine & Blisters

- Defenders:
  - 4 SPOs – At blisters
  - 3 ASOs – At ECP
  - 1 RTL, 1 CAS – In CAS
- Adversaries
  - 5 Attackers
  - 1 Cyber-attacker
  - 1 Insider
    - Provides cypher codes for shark cage doors

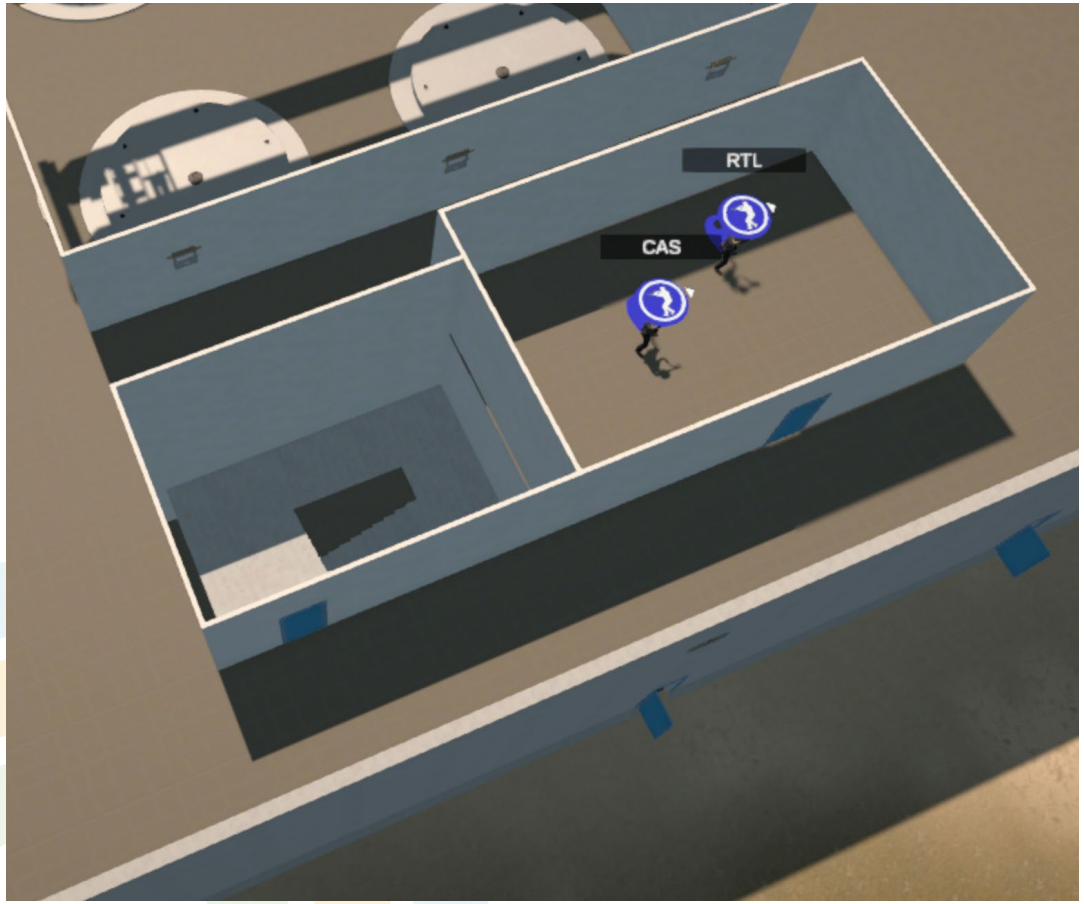


iPWR Facility - Results

- The cyber attacks did not result in an adversary win because:
  - Task times are too high (5000s)
  - Blister BBRE's are inherently defensive
  - Mezzanine gun ports force adversaries to focus attack on eliminating entire defense team
- Even assuming the adversaries enter the building undetected does not result in a win.



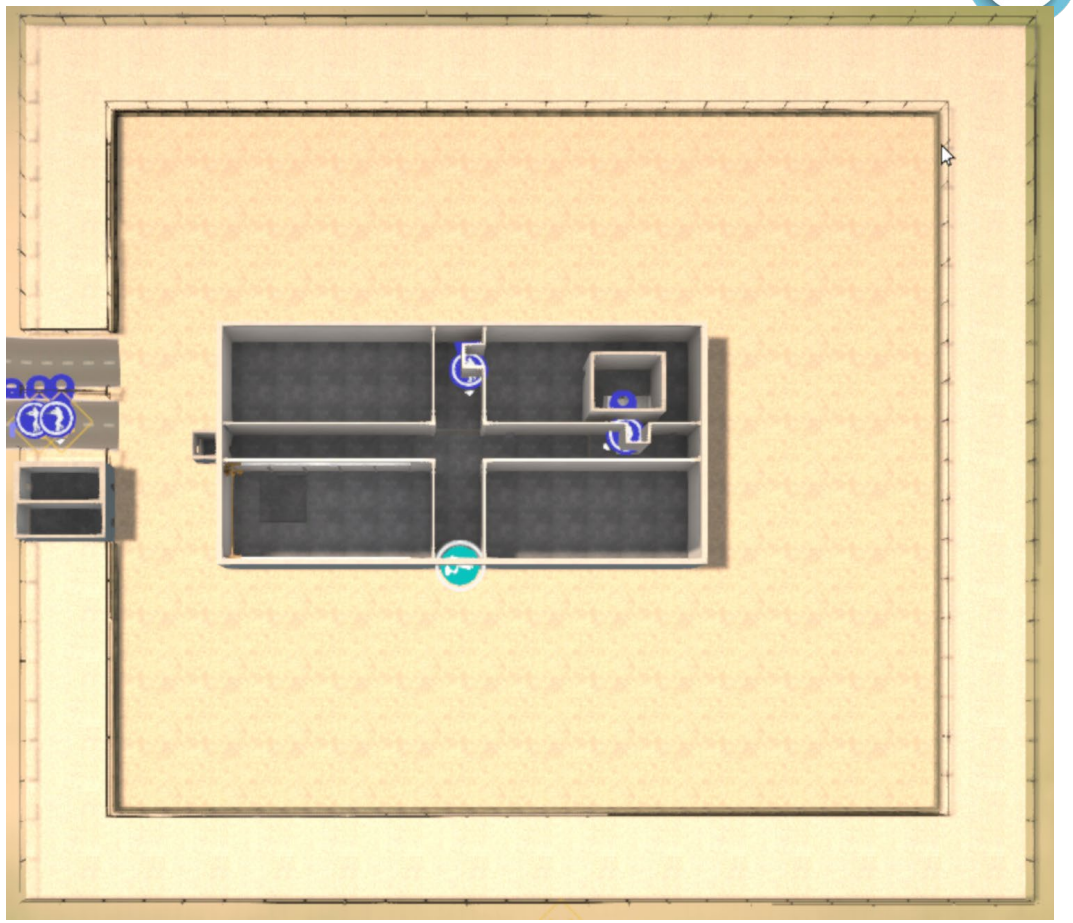
iPWR Facility – Lessons Learned



- Adversaries are funneled into the stairwells to the mezzanine especially the stairs next to CAS.
- Enhancing the security posture on this stair well and door would completely prevent adversary success possibilities.
  - Gun ports from CAS to stair well.
  - Gun ports from mezzanine to stair well
  - Grenade screening in hallway around door
  - Shark cages on stairwell doors from shipping/recieving

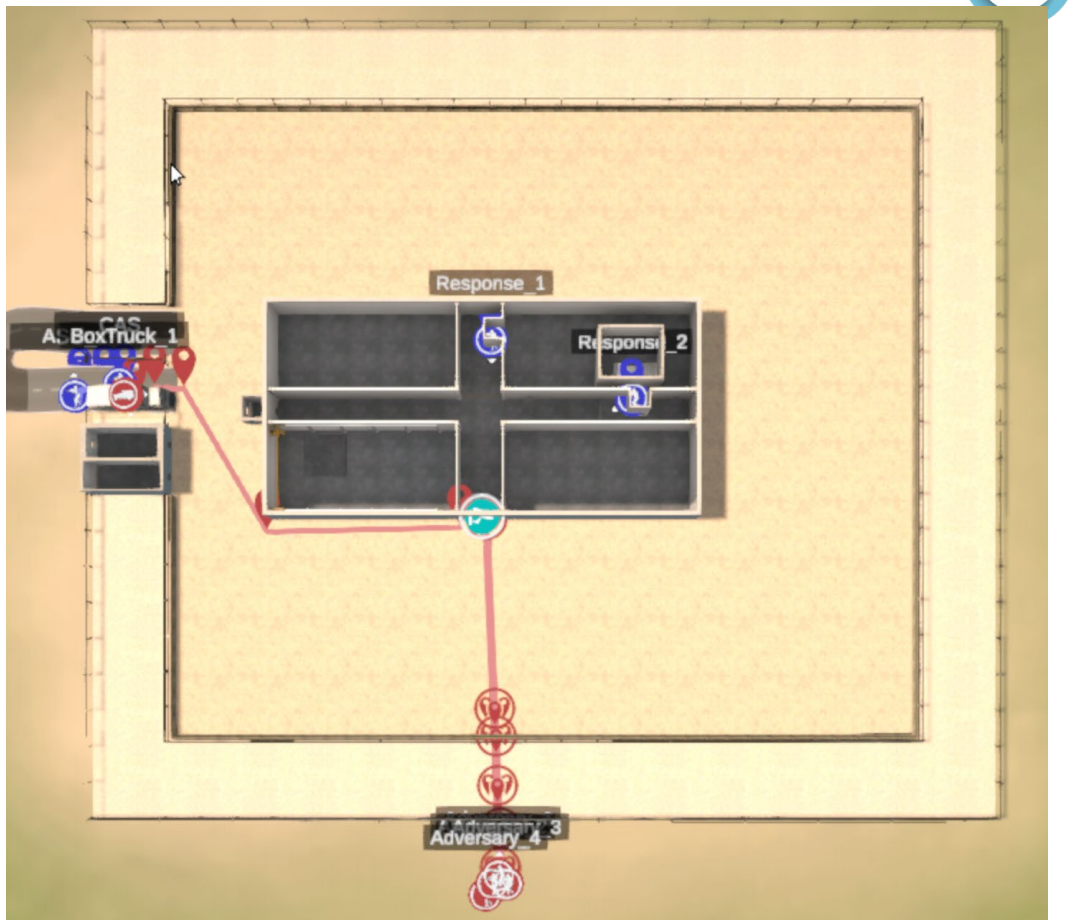
Micro Reactor Facility

- Defenders:
  - 2 SPOs – At defensive positions
  - 1 ASO – At ECP
  - 1 CAS, 1 RTL – In CAS
- Adversaries
  - 5 Attackers
  - 1 Cyber-attacker
  - 1 Insider
    - Provides cypher codes for shark cage doors



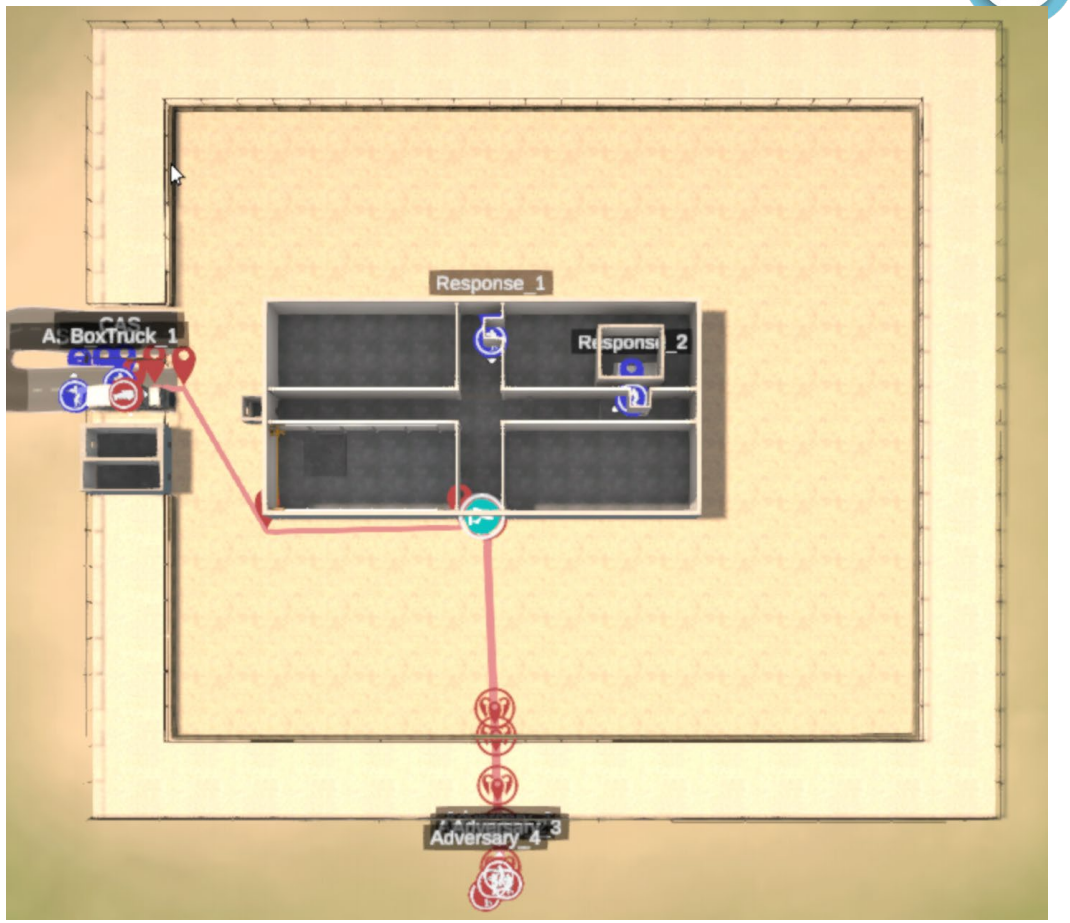
Micro Reactor Facility - Results

- Adversaries win if using vehicle distraction to lure CAS outside.
  - Does not require cyber attack depending on local rules of engagement
  - Cyber attack offers higher probability of adversary success.



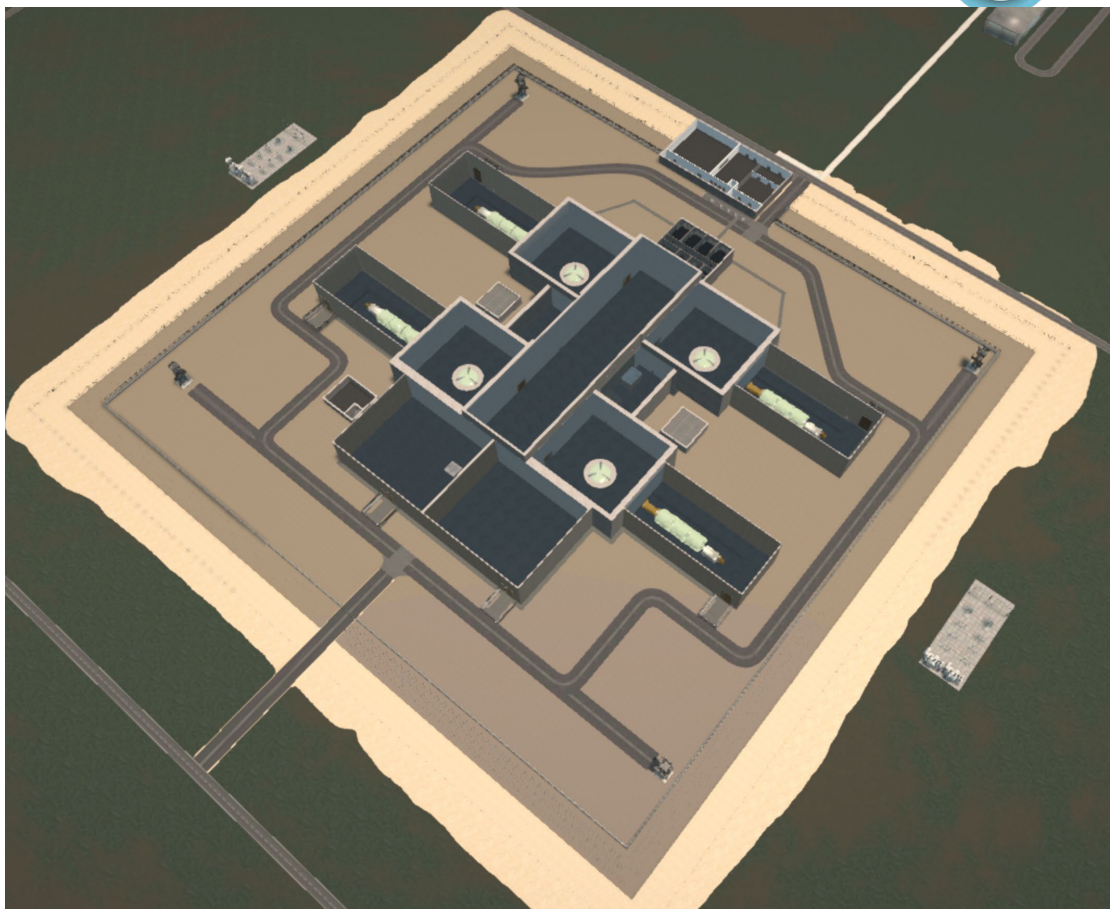
Micro Reactor Facility - Lessons learned

- Shark cages on doors result in adversary loss
  - Adversary depends on using explosives thrown into building
- Facility defense is heavily reliant on task time length and offsite response time.



SMR Facility

- Defenders:
  - 4 SPOs – In towers
  - 5 SPOs – Roving
  - 3 ASO – At ECP
  - 1 CAS, 1 RTL – In CAS
- Adversaries
  - 5 Attackers
  - 1 Cyber-attacker
  - 1 Insider
    - Provides cypher codes for shark cage doors

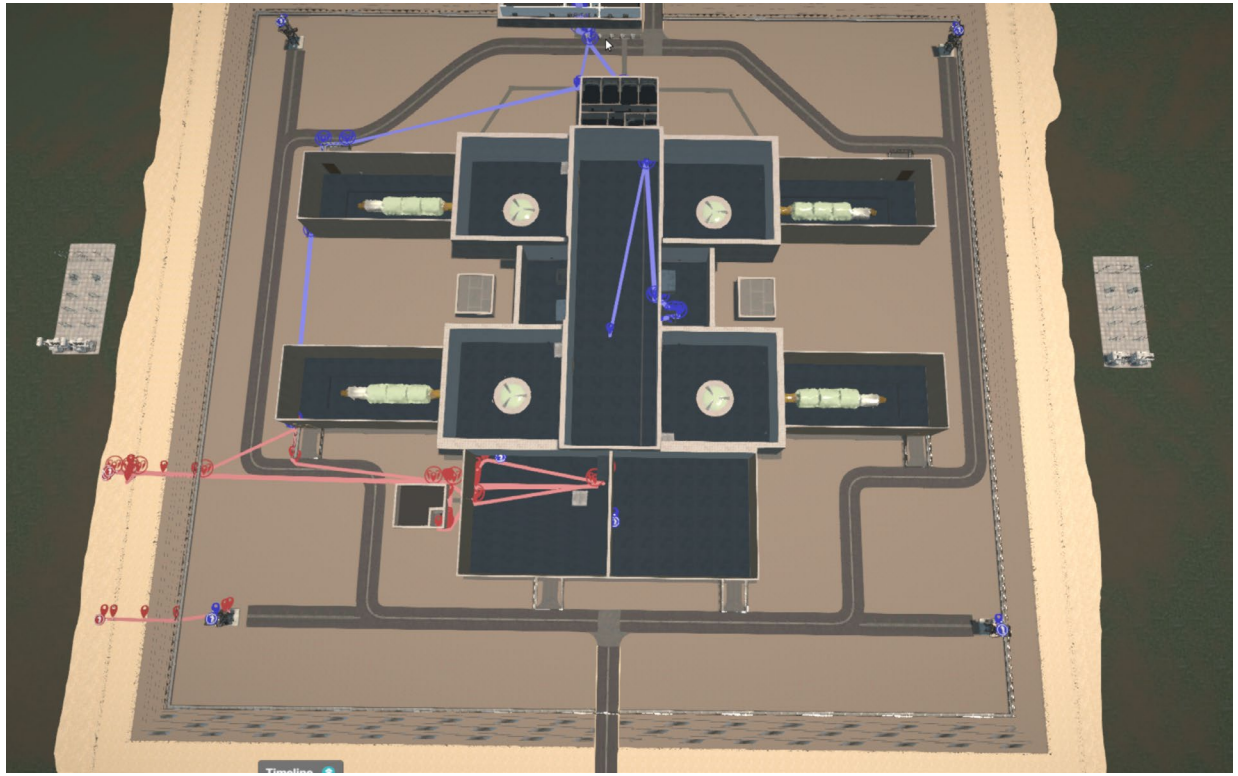


SMR Facility - Results

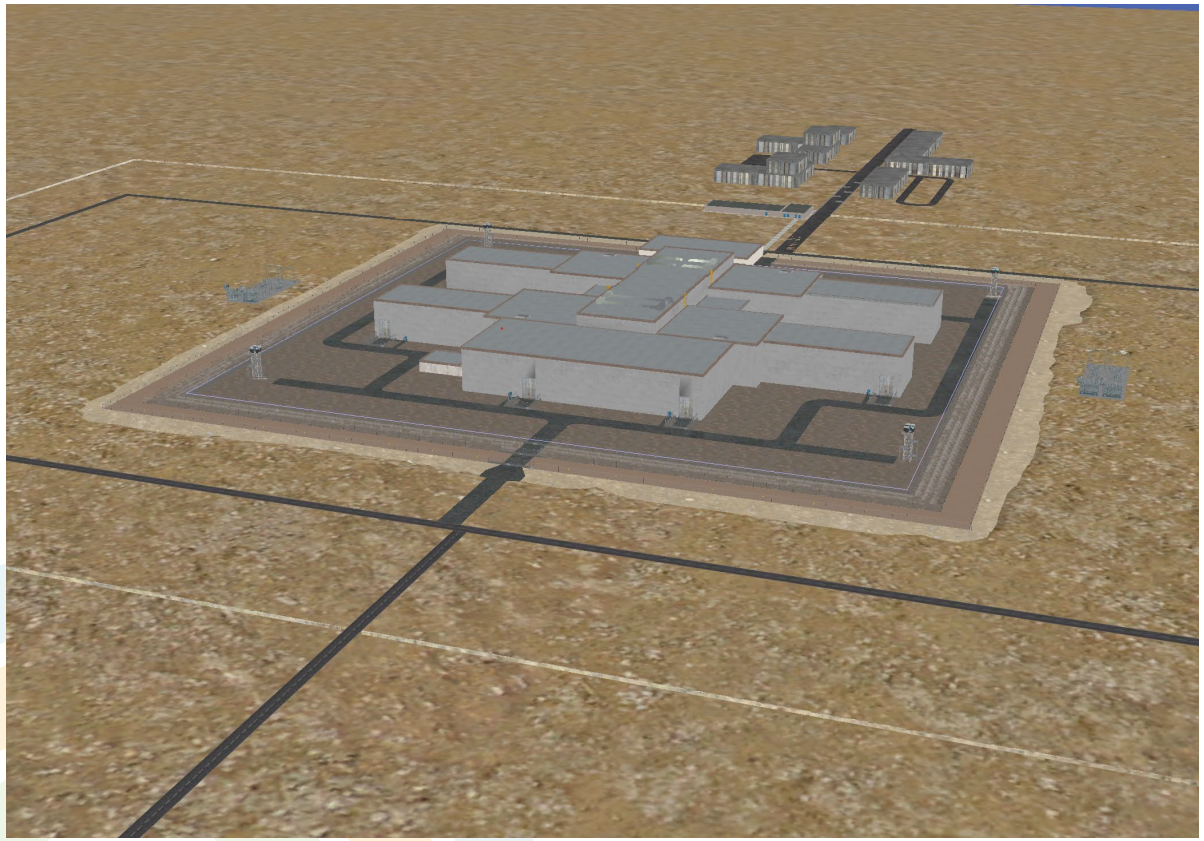
No PIDAS	Badge Access	No Cameras	Outcome
X			Blue win; Adv reaches target
	X		Blue win; Adv reaches target
		X	Blue win
X	X		Adv win
X		X	Adv win
	X	X	Blue win
X	X	X	Adv win

SMR Facility – Lessons Learned

- Facility resembles more conventional designs.
- Requires 2 cyber attacks to be successful.
- Adversaries reach targets with only 1 cyber attack, resulting in fire fight at storage pool.
- Towers do not provide a significant advantage at this facility without the PIDAS.
- Applying DCSA to this design would significantly reduce adversary likelihood of success.



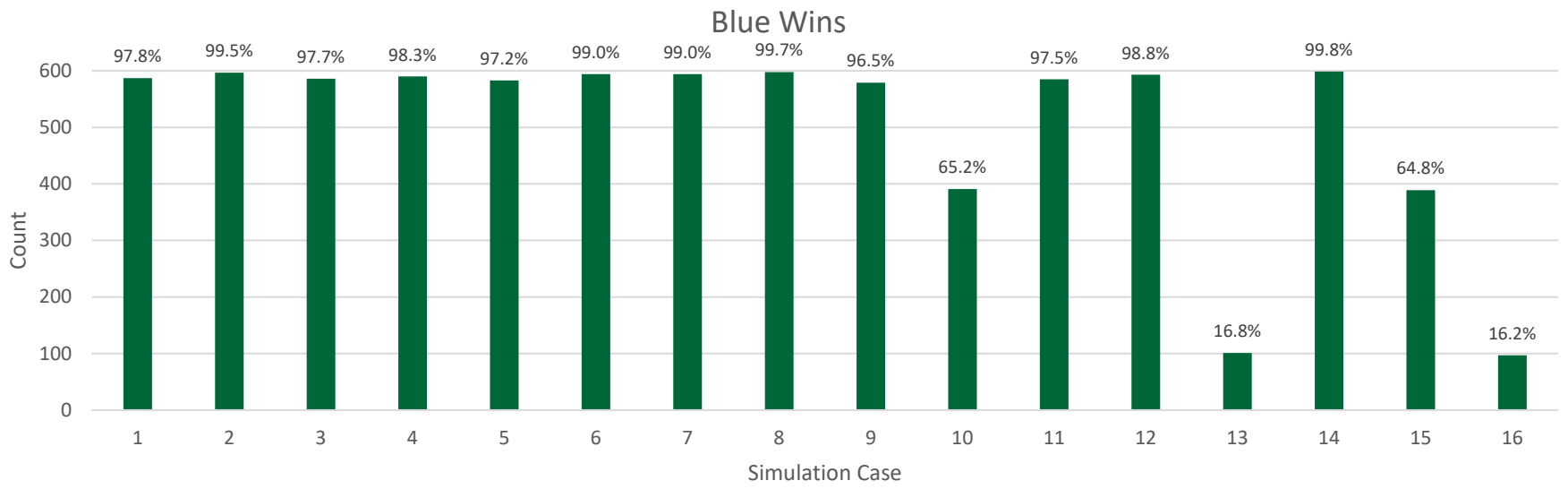
Dante Cyber Analysis



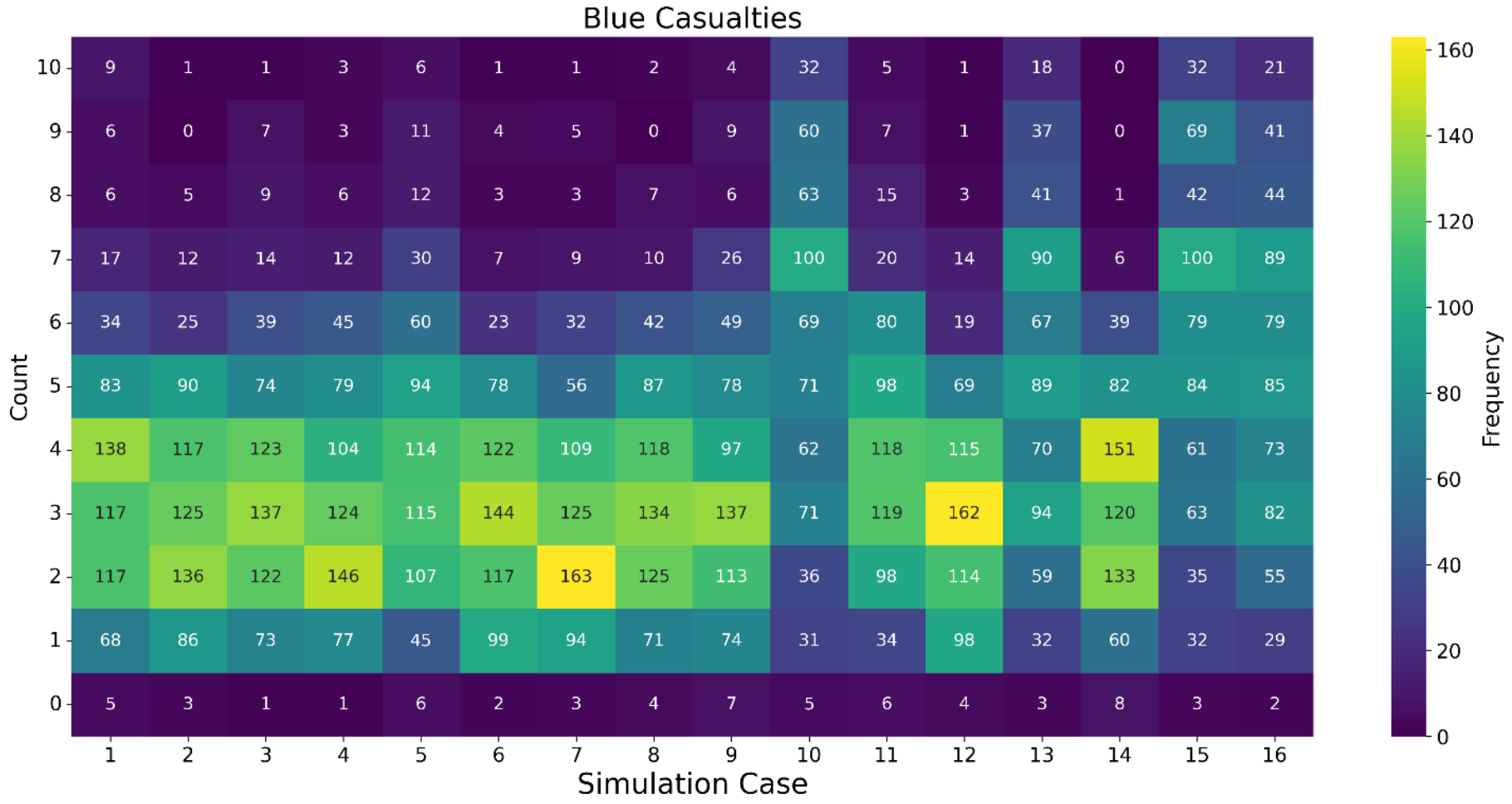
- Dante Cyber World
  - Allows cyber effects to influence the simulation.
  - I.E., camera spoofing, sensor disabling, door lock defeats, access control manipulation.
- Notional NRC SMR site selected to run analysis.
  - Sabotage scenario will be used to evaluate the performance of PPS under cyber attack.

Cyber Risk Analysis: Results

Digital System Attacked	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Door Sensors (X1)		X				X	X	X				X	X	X		X
Cameras (X2)			X			X			X	X		X	X		X	X
Motion Detector (X3)				X			X		X		X	X		X	X	X
Fence Sensors (X4)					X			X		X	X		X	X	X	X



Cyber Risk Analysis: Results (cont.)



Cyber-Physical Milestones

- Cyber Physical TTX
  - ✓Full series of TTXs complete
  - Milestone report to start in June
- Simulation Driven Tiered Cyber Analysis for Physical Protection Systems
  - Dante modifications to be completed in June
  - Data analysis pipeline started
  - Milestone report to start in July

Questions

DCSA – PPS Linking

The Defensive Cyber Security Architecture methodology offers a risk-informed performance-based defense-in-depth approach for control systems which could be applied to Physical Protection Systems.

- Requires characterizing the risk on the facility given system degradations due to cyber attack.
- This characterization on the PPS requires developing statistical models of the performance impact of cyber attacks.
- Dante was selected to model the performance of the PPS with cyber degradations.

Modeling System Effectiveness with Dante

Dante is a design and analysis tool specific to physical security.

- Models adversary attacks and the security response **according to policy**
- Includes models of **delay elements, sensors, comms,** and command-and-control behaviors of **responders**
- Internally conducts **dynamic path analysis and lethality effects**
- Results used to **Compare changes in site security** (e.g. upgrades, manpower)
- **Accredited** by OSD/DTRA for DoD use
- **Users:** NATO, DTRA, USSS, AF, OGAs

Dante Analysis Process

Planning

Evaluate Physical Security

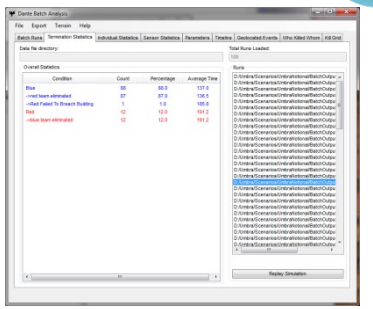
- Concept of Operations (CONOPS)
- Tactics, Techniques and Procedures (TTPs)
- Weapons Systems
- Protective systems (barriers, fences, sensors)

Dante Scenario Setup

Setup using Dante Scenario Editor

- Define up to 3 different sides
- Create assets for each side
- People, weapons, platforms, sensors
- Create actions for each side (TTPs)

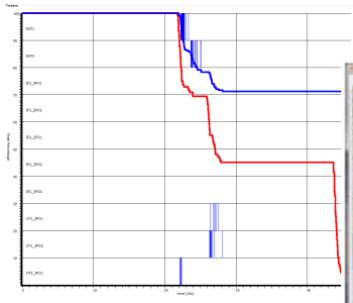
Execution



Execution Mode

- Interactive
- Monte Carlo Analysis
- Scenario Replayer

Statistics & Scenario Replay



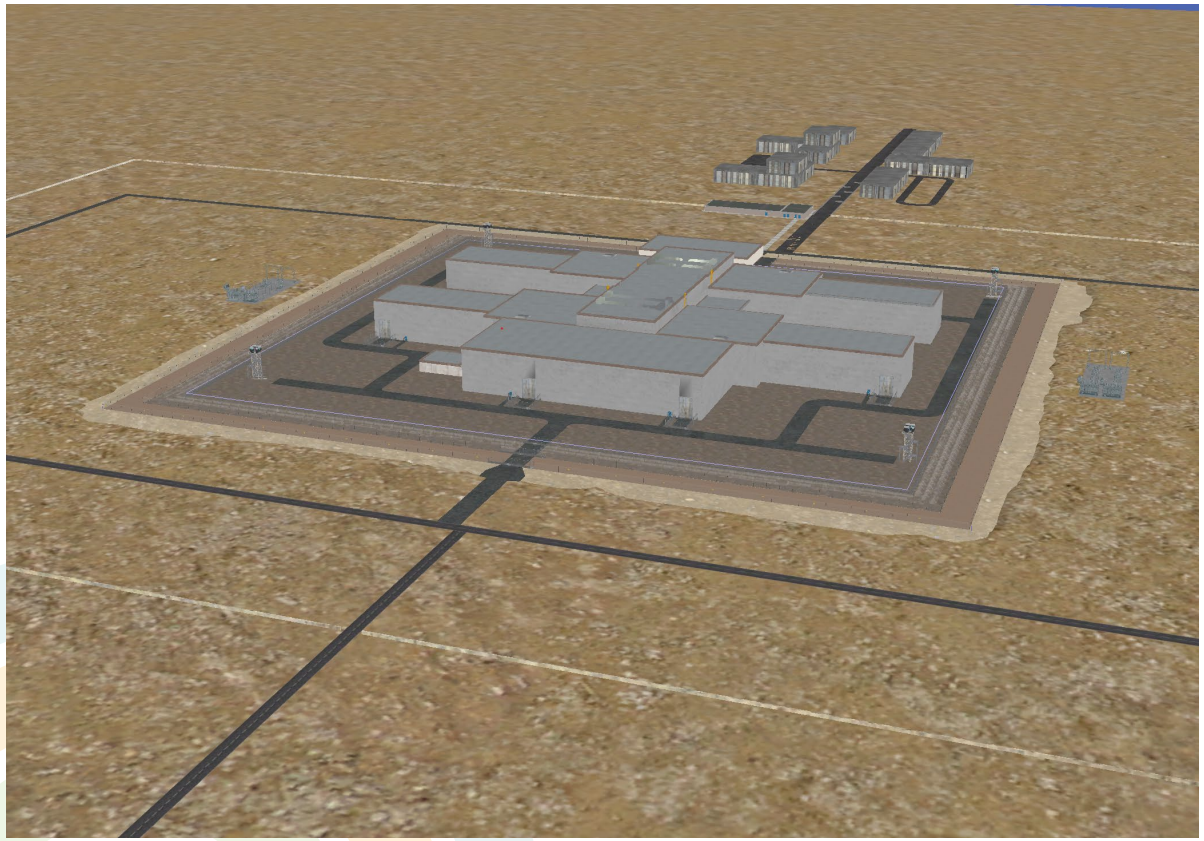
Batch Statistical Analysis

- Provide insights into “key” players and events
- Who Killed Whom, When, Where and with what statistical distribution
- Supports probability of neutralization computation

Behavioral Response Example

Tasking, Sensing, & Behavioral Response

Dante Cyber Analysis



- Dante Cyber World
  - Allows cyber effects to influence the simulation.
  - I.E., camera spoofing, sensor disabling, door lock defeats, access control manipulation.
- Notional NRC SMR site selected to run analysis.
  - Sabotage scenario will be used to evaluate the performance of PPS under cyber attack.