SAND2022-7656C

Sandia National Laboratories

Performance Testing of Cyber Incident Response at Nuclear Power Plant Operators

Nuclear Energy Safety Technology

Presented by Michael T. Rowland

Prepared by Andrew S. Hahn

SAND2022-XXXX

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.

Outline

Objectives
- Overall R&D Objective
- Hypothesis Overview

Functional Exercise
- Overview
- Exercise Setup

Blended Attack Experiment
- Objectives & Challenges
- Experiment Site
- Experiment Setup
- Development Timeline

Future Development

Closing Remarks

Photo by: Bonnie Bos

Overall R&D Objective

Research Objectives

1. Investigate how cyber-attacks manifest themselves; especially those associated with Blended Attacks.
2. Provide insights into the abilities needed to respond to the attack; and
3. Identify a potential methodology to evaluate overall level of preparedness to protect against blended attacks.
   - For example, examine the communications and coordination between physical and cyber security teams to respond to blended cyber-physical attacks requiring a coordinated physical and cyber response. Accordingly, this is referred to as a blended cyber security incident response exercise.

Functional Exercise Objective

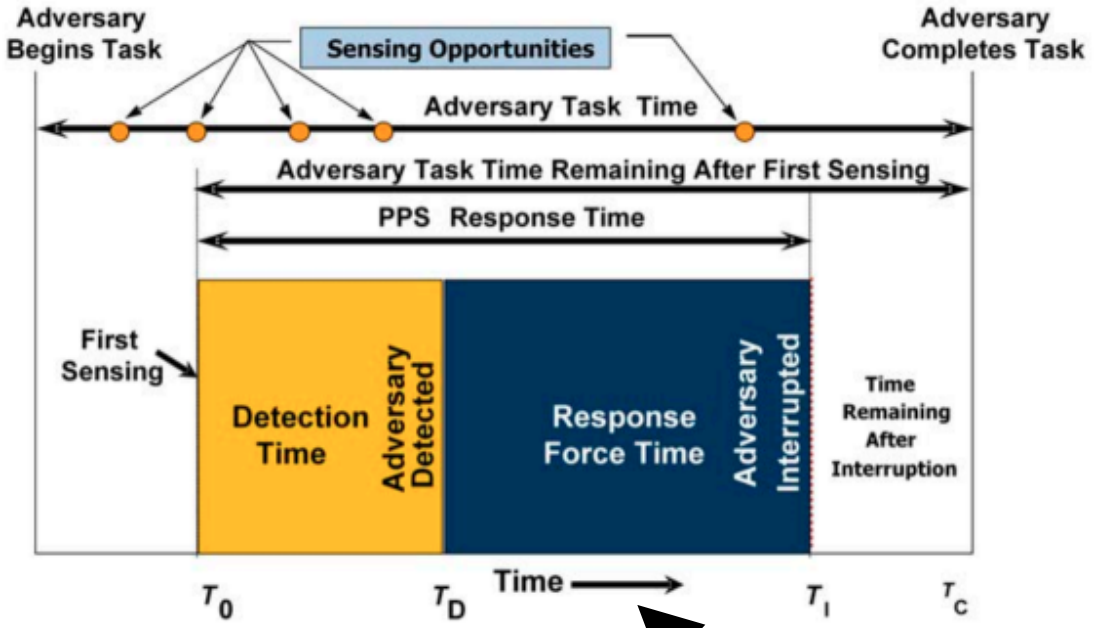
The outcome of the event is the collect and analyze empirical data to support the methodology developed by CNL to derive performance criteria (time, quality, accuracy) which allows evaluation of an organization's capability to provide an effective blended attack response.

Blended Attack Experiment Objective

This experiment will measure evaluate the coordination and response to blended cyber-physical attacks. The data collected will provide insight into the nature of blended attacks and aid in the development of defensive strategies.

Hypothesis Overview

Physical Protection (IAEA NSS27-G)



Cyber Security (BSI 100-4)

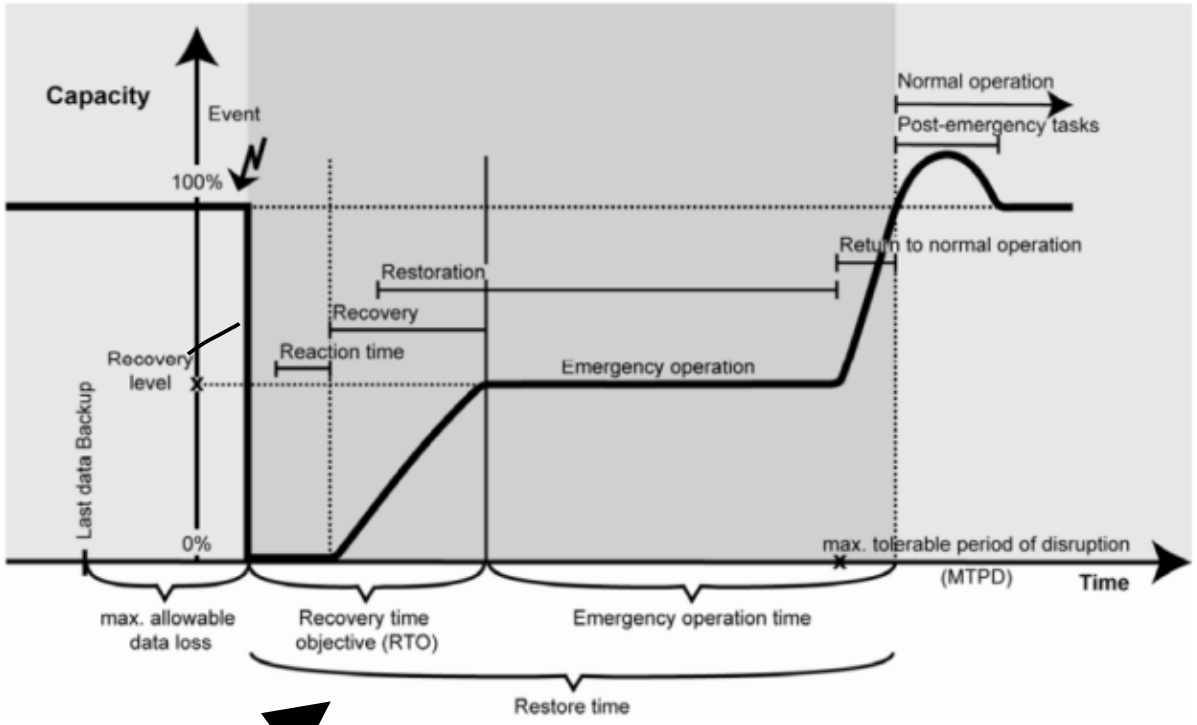


Figure 6: Recovery parameters

Set of Observations

Functional Exercise Overview

Scenario

- A malicious insider installs a remote shell USB device on a firewall maintenance computer and identifies an open vendor maintenance port to a lower security levels.
- Insider steals an engineering laptop and uses it to setup a remotely activated attack through the identified open port. This disrupts the operation of the steam generator level controller.

Players

- Cyber Security Operations Center (Cyber SOC)
- Maintenance & Operations

Lessons Learned

- Exercise staging area was critical to orchestrating the exercise
- Communications need to be streamlined and rapid for actor co-ordination
- Cyber injects need systematic deployment
  - Cyber SOC operators experience significant timing delays between injects and Cyber SOC detection that are not acceptable during exercises
- Cyber injects are complex and need a better co-

Photo: Canadian Nuclear Laboratories

Functional Exercise Setup

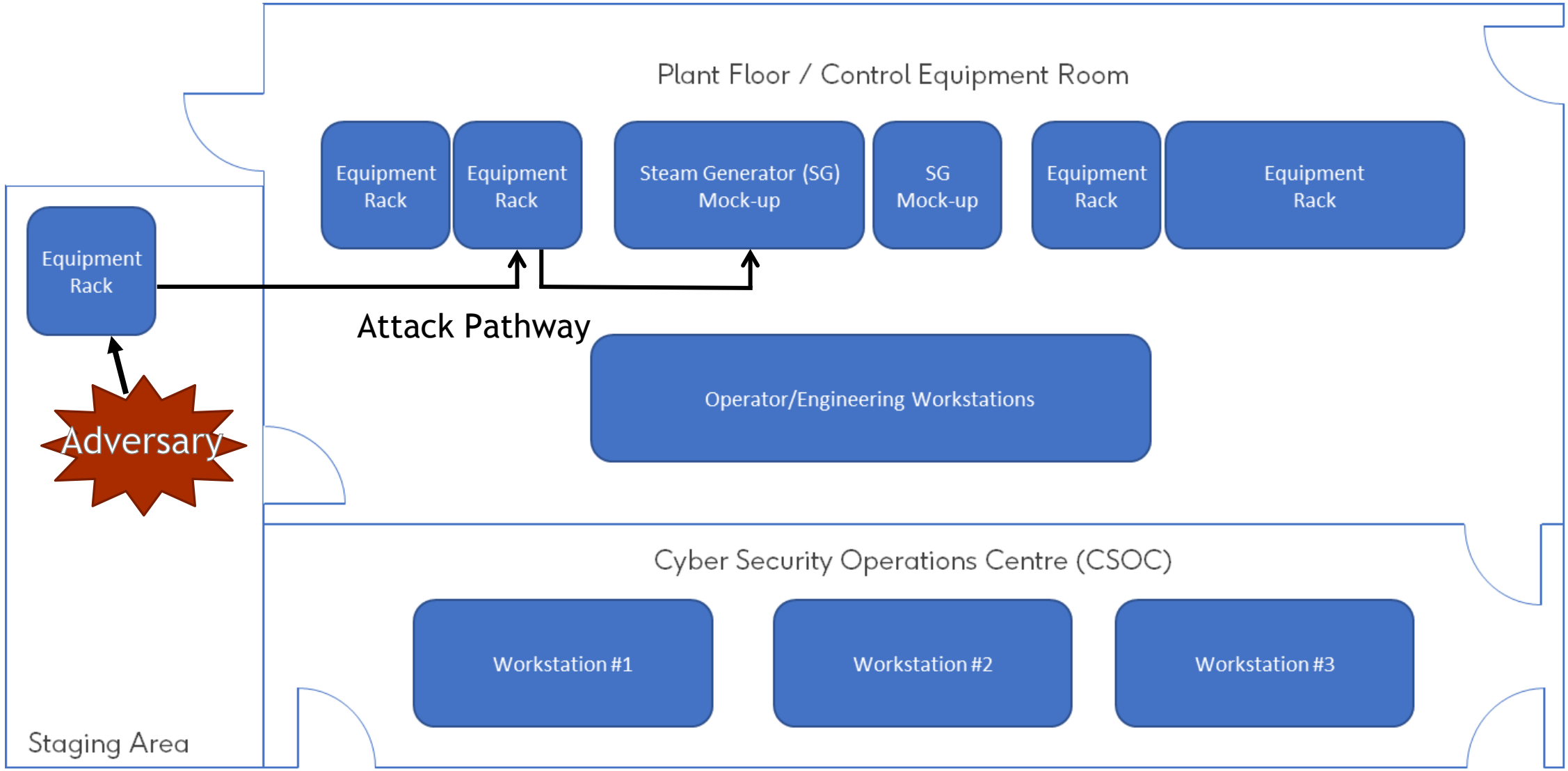


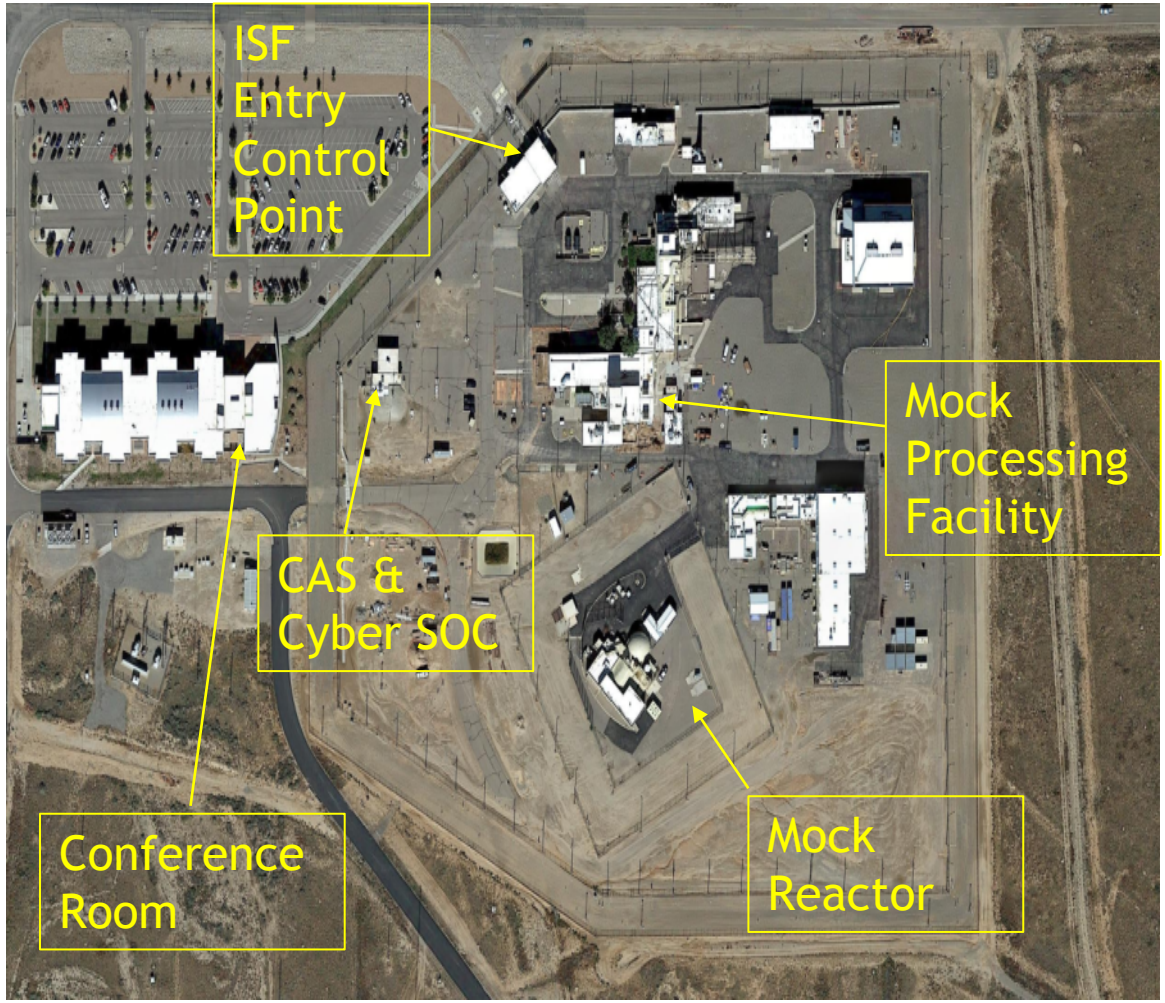
Diagram courtesy of Canadian Nuclear Laboratories

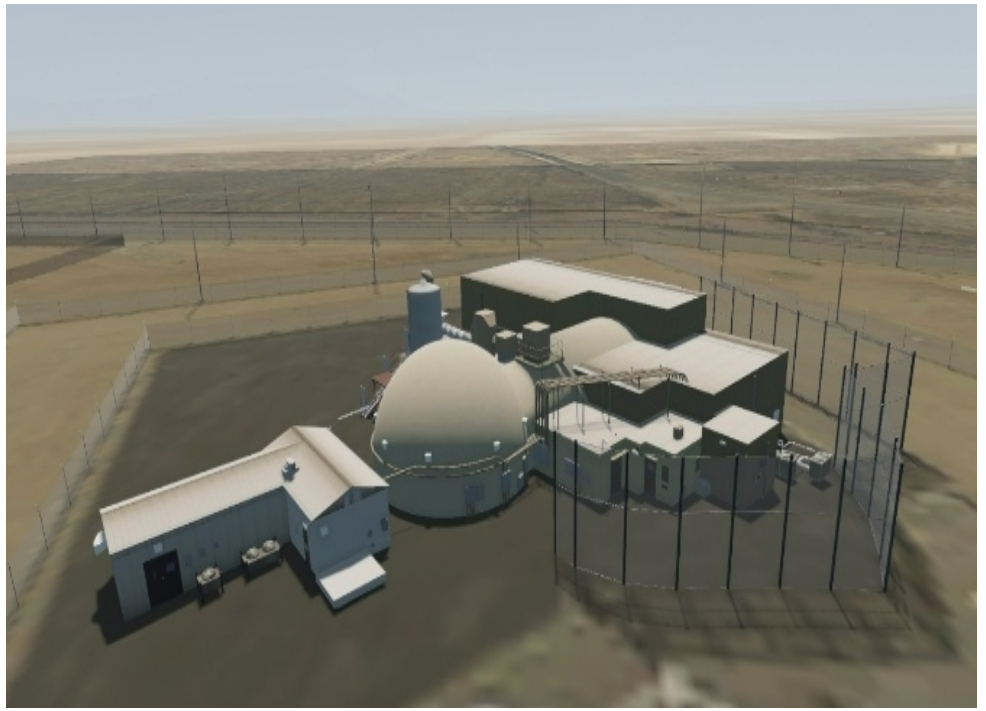
Blended Attack Experiment Objectives and Challenges

The purpose of exercises is to improve an organization's response to an event, this experiment will test a hypothesis on the nature of cyber attacks. The goal is to discover fundamental principles that aid in defense against cyber-physical attacks.

Objective #1	**Investigate how cyber-attacks manifest themselves; especially those associated with Blended Attacks.**
Challenges	"Live" Exercises involving Blended Attacks have never been performed
	Very limited data is available on how cyber-attacks manifest themselves in PPS
	Previous experiments did not support an actual Tactical intrusion
Objective #2	**Provide insights into the abilities needed to respond to the attack**
Challenges	Exercises involving Blended Attacks have never been performed
	Experiment environments have not previously been detailed or constructed
Objective #3	**Identify a potential methodology to evaluate overall level of preparedness to protect against blended attacks.**
Challenges	No existing "blended" theory or research to support methodology to support identification of criteria
	Without the methodology, efficient design and construction of experiment environments will be challenge

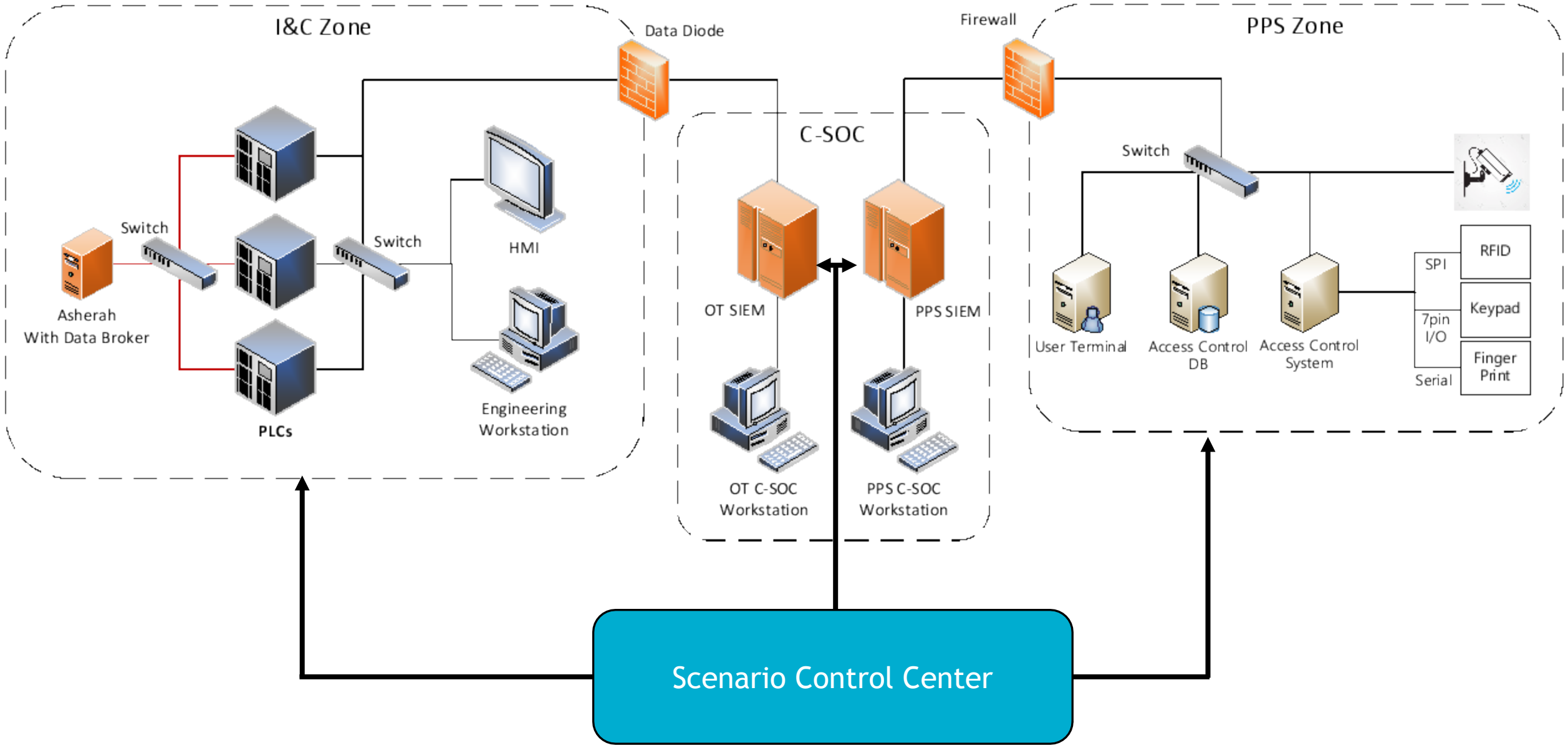
Blended Attack Experiment Site





- Asherah Simulator – Located within the Mock Reactor
- Cyber SOC and CAS – Co-Located in Same Building
- Scenario Control Center – Located in SAS
- Computer Animated Fly Over Video
  - https://youtu.be/ghDiyNF4Hks

Blended Attack Experiment Setup



Blended Attack Experiment Development Timeline

#	Meeting	Date	Location	Status
1	Project Kick Off Meeting	25th – 28th October, 2021	SNL	Completed
2	November Fredericton Trip	29th November – 3rd December, 2021	CNL	Completed
3	Cyber Exercise at CNL	7th – 10th March, 2022	CNL	Completed
4	Agreement on the Project Plan Selection of Candidate Scenarios	2nd – 6th May, 2022	SNL	Planning
5	Methodology Review	13th – 16th June, 2022	Virtual	Planned
6	Final preparation meeting before the Dry Run	17th – 21st October, 2022	SNL	Planned
7	The Dry Run	20th – 24th February, 2023	SNL	Planned
8	Signature Event	15th – 19th May, 2023	SNL	Planned

Closing Remarks

- Sandia National Laboratories in collaboration with the Canadian Nuclear Laboratory and Idaho National Laboratory are developing an experiment to evaluate the hypothesis that cyber security event timelines have similarity to physical security events.
- Sandia National Laboratories is establishing a experimental testbed that can evaluate cyber physical blended attacks and their response

End