SAND2022-3028C

Sandia National Laboratories

A Cyber-Physical Experimentation Platform for Resilience Analysis

Presented by Jamie Thorpe (jthorpe@sandia.gov)

Authors: Jamie Thorpe, Ray Fasano, Meghan Galiardi Sahakian, Amanda Gonzales, Andrew Hahn, Joshua Morris, Timothy Ortiz, Hannah Reinbolt, Eric D. Vugrin

ACM Workshop on Secure and Trustworthy Cyber-Physical Systems

Baltimore-Washington DC Area

April 27, 2022

U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration

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

- Motivation
- Platform Overview
  - System Representation
  - Threat Representation
  - Metrics
  - Experiment Control
- Nuclear Power Use Case
- Results
- Conclusion

Motivation

Colonial Pipeline (Darkside): 2021

Iranian Centrifuges (Stuxnet): ~2010

Ukrainian Power Grid (CrashOverride): 2015, 2016

Chemical Facility Safety Systems (HatMan): 2017

Industrial control systems are increasingly being targeted by cyber attacks.

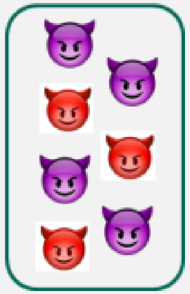
Key Questions

How should infrastructure operators prioritize cyber threat planning?

How can we model cyber attacks and systems to inform prioritization and characterize resilience of critical infrastructure systems?

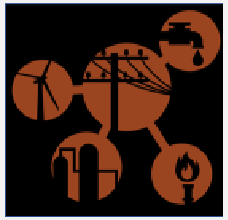
Can we address these questions in a way that is reliable and gives quantitative, meaningful results?

ADROC: Advancing the Resilience of Control Systems

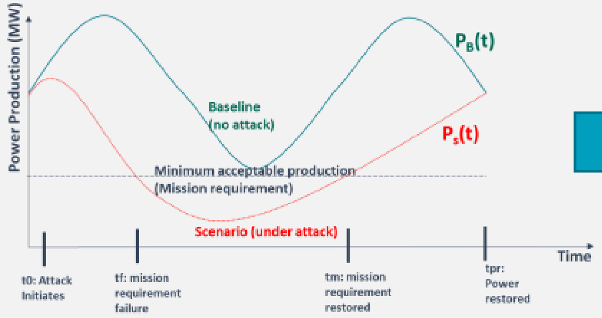


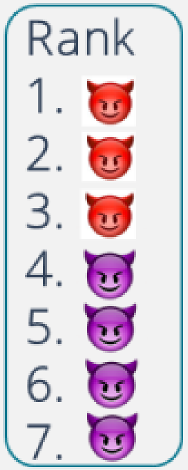
Parameters

CALDERA



Effects





INPUTS: Threats

Threat Emulation

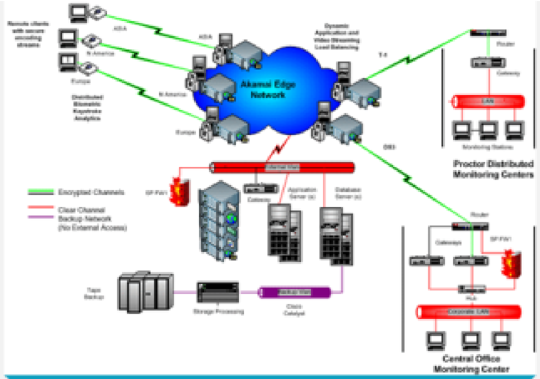
Emulated Industrial Control System

Outputs: Consequences & Metrics

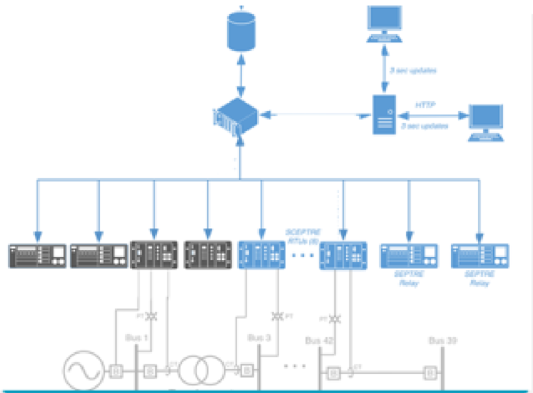
Four Components

- Representation of Industrial Control System
- Representation of Threat(s) of Interest
- Experiment Control
- Metrics

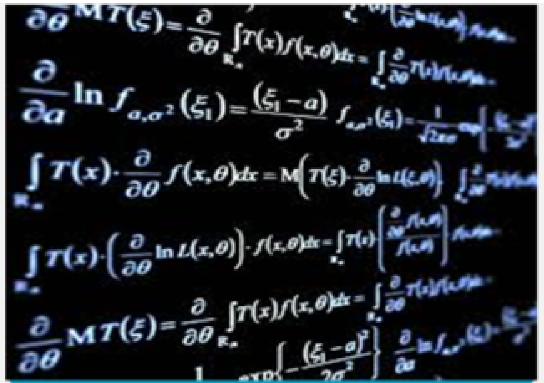
Representation of Industrial Control Systems



ACTUAL SYSTEM



VIRTUALIZED TESTBED



SIMULATION

"BAD DAY" BRAINSTORMING

Increasing Realism
Decreasing Flexibility
Increasing Cost
Increasing Time

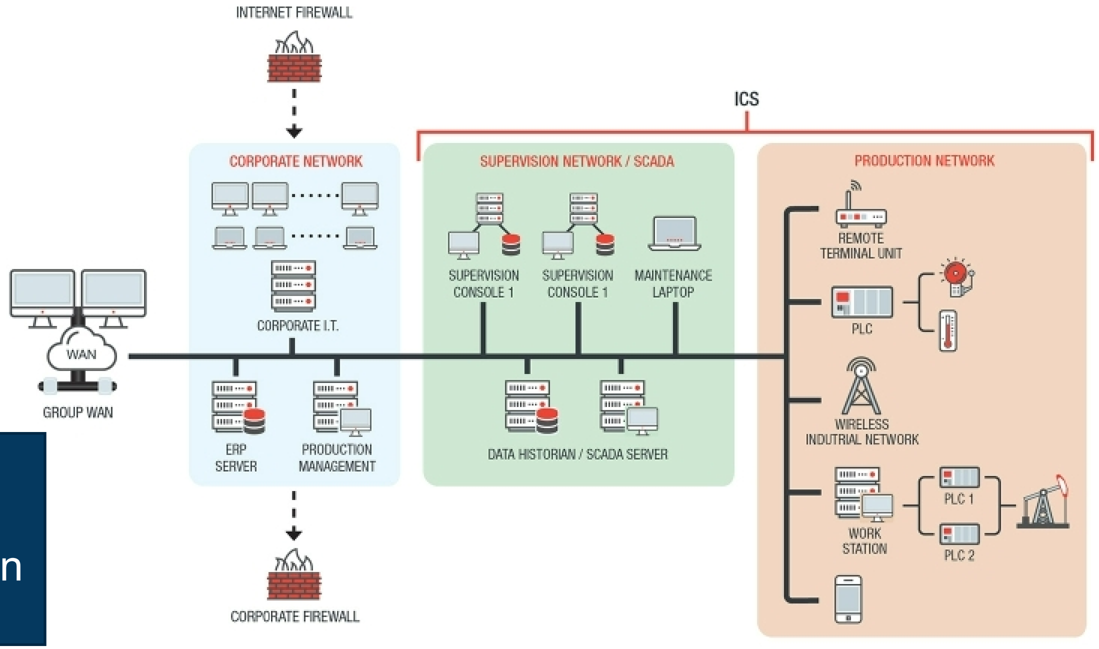
Increasing Abstraction
Increasing Flexibility
Decreasing Cost
Decreasing Time

We have several options for modeling and analyzing cyber threats.

Representation of Industrial Control System

Experiment Control

SCEPTRE



Threat Representation

The ADROC Platform Leverages SCEPTRE for ICS Emulation and Integrates Threat Emulation Capability.

Representation of Threats

Several tools available to model threats in a high-fidelity, automated way

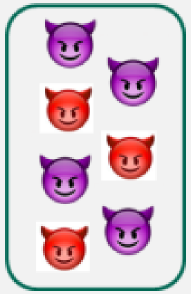
CALDERA is a MITRE-developed threat emulator

- Attack profile, including capabilities and goals
- Automated
- Closely tied to MITRE ATT&CK framework
- Opportunity to add plug-ins

The ADROC Platform Integrates CALDERA with SCEPTRE and Extends CALDERA with ICS-Targeted Threats.

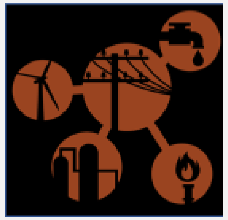
Experiment Control

Expt. Control & Metrics: RevRun

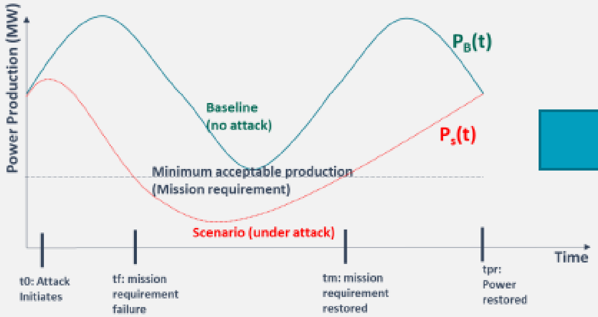


Parameter
s

CALDERA



Effect
s



Rank

1.
2.
3.
4.
5.
6.
7.

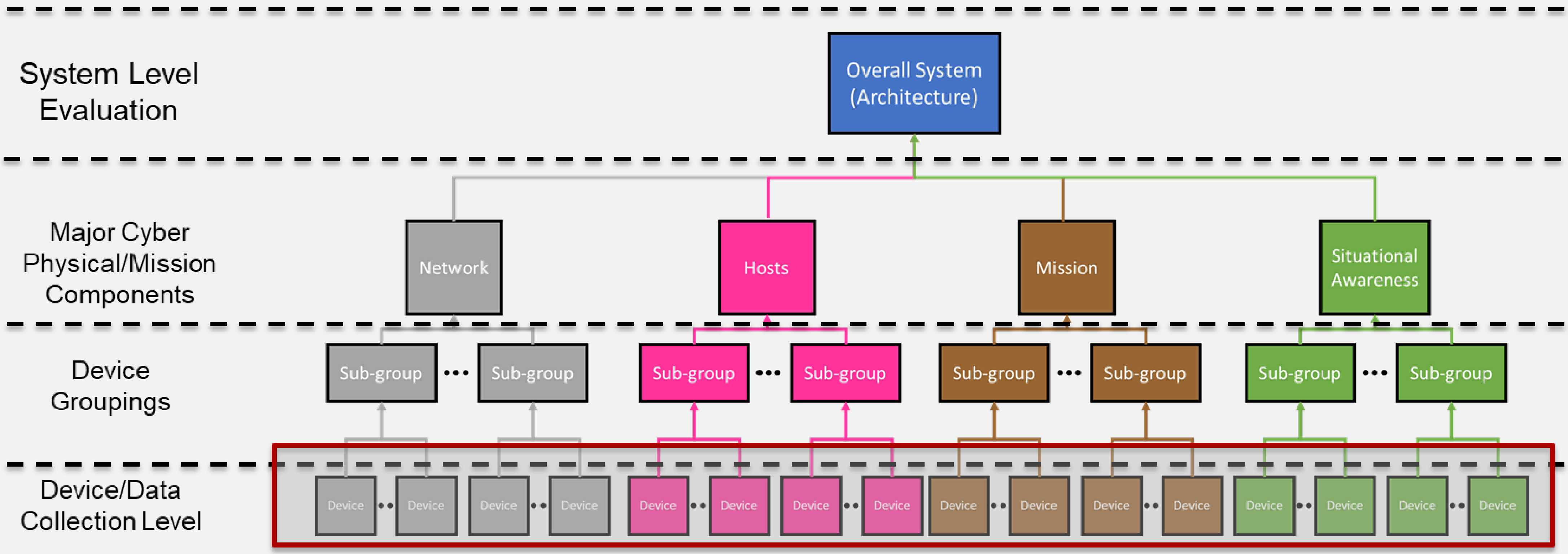
INPUTS:
Threats

Threat Emulators:
CALDERA & ManiPIO

Emulated System:
SCEPTRE

Outputs:
Consequences & Metrics

Metrics



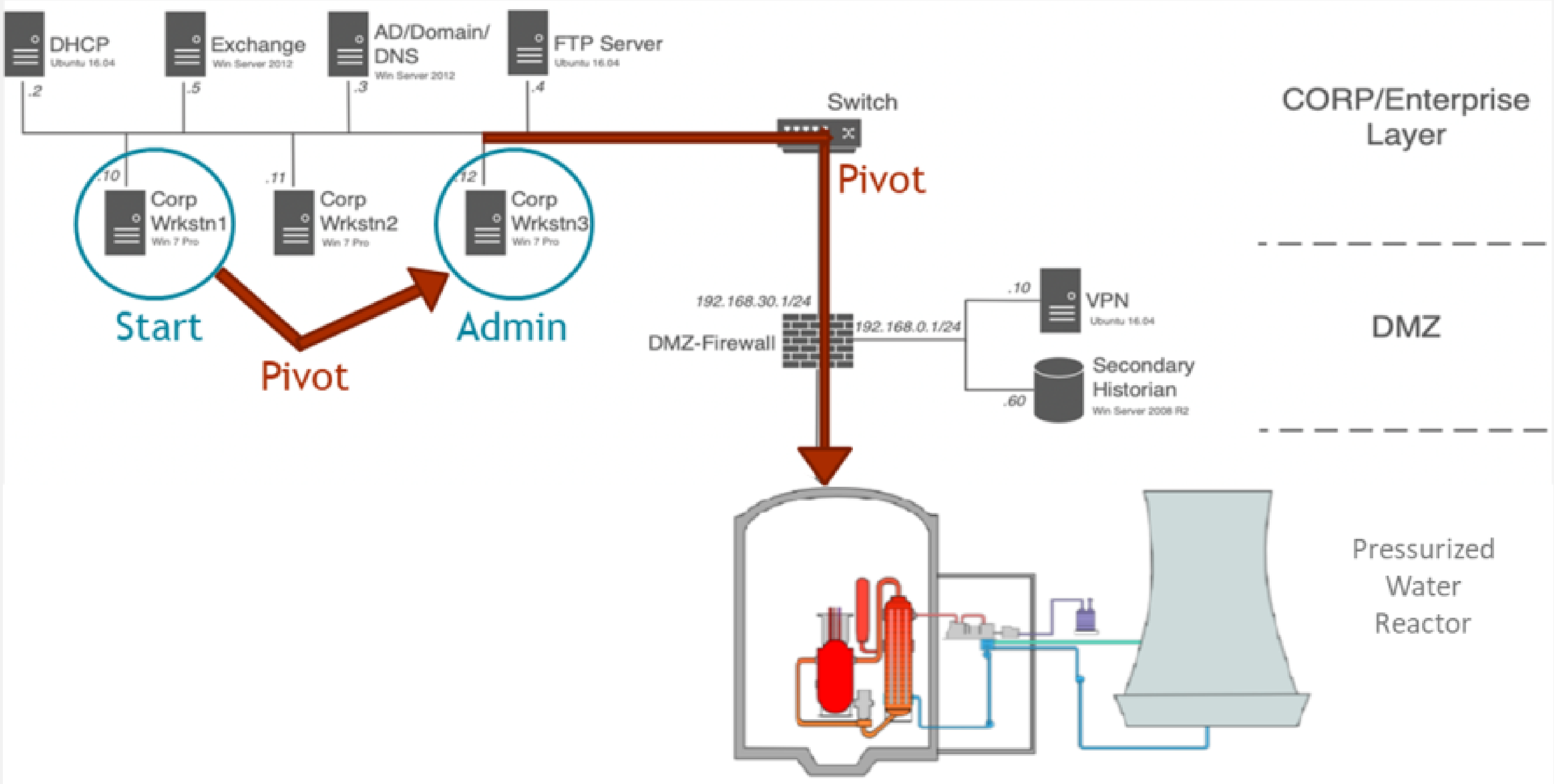
The Resilience VeRification Unit (RevRun) contains an extensible library of resilience metrics for analyzing emulation results.

Use Case

System: Pressurized Water Reactor for Nuclear Power Generation

Threat: Worm from the Corporate Network Performs Data Injection

Scenario: Attack on Nuclear Power Plant



Attacker Goal: Cause Unsafe Conditions in the System

Attack Specification

Scenario #	Corporate Network: Attack Path	SCADA Network: Target & Effect
0	N/A	N/A
1	Full path	RCP PLC: set speed to 0 → overheat core
2		SG PLC: set valve position to 0→ increase pressure, overheat core
3		RCP & SG PLC: change set point in RCP PLC & provide constant sensor reading into SG PLC
4		RCP PLC: mimic broken sensor by toggling flow value between 0 and 100
5	Min path	RCP PLC: set speed to 0 → overheat core
6		SG PLC: set valve position to 0→ increase pressure, overheat core
7		RCP & SG PLC: change set point in RCP PLC & provide constant sensor reading into SG PLC
8		RCP PLC: mimic broken sensor by toggling flow value between 0 and 100

RCP = Reactor Coolant Pump SG = Steam Generator PLC = Programmable Logic Controller

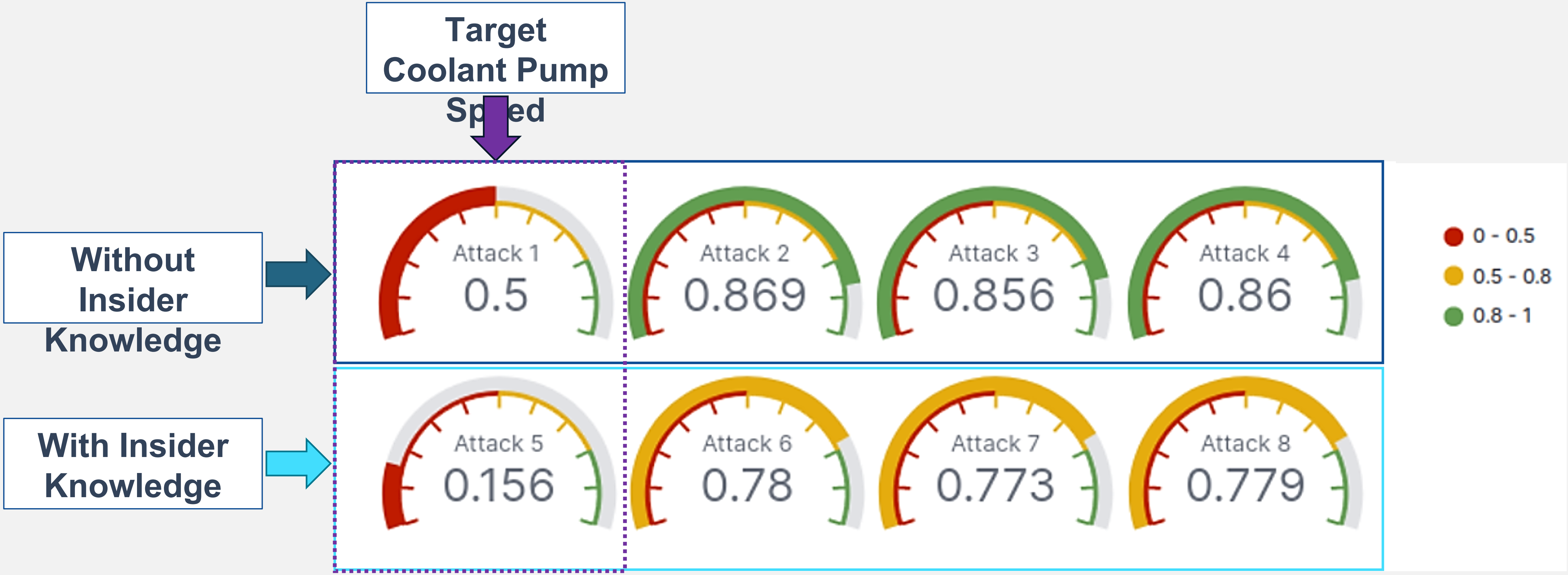
Metrics of Interest

Data Source	Metric
Pressure	1st time pressure exceeds 8.974 MPa *
Reactor Core Temp	1st time temp exceeds 580K *
DNBR	1st time DNBR drops below 1.3 *
PWR Coolant Flow	Cumulative diff between nominal and attack values
Traffic between C2 server and privileged device	Cumulative packet count
Traffic between C2 server and SCADA Workstation	time 1st packet is sent

***Triggers Reactor Protection Scheme**

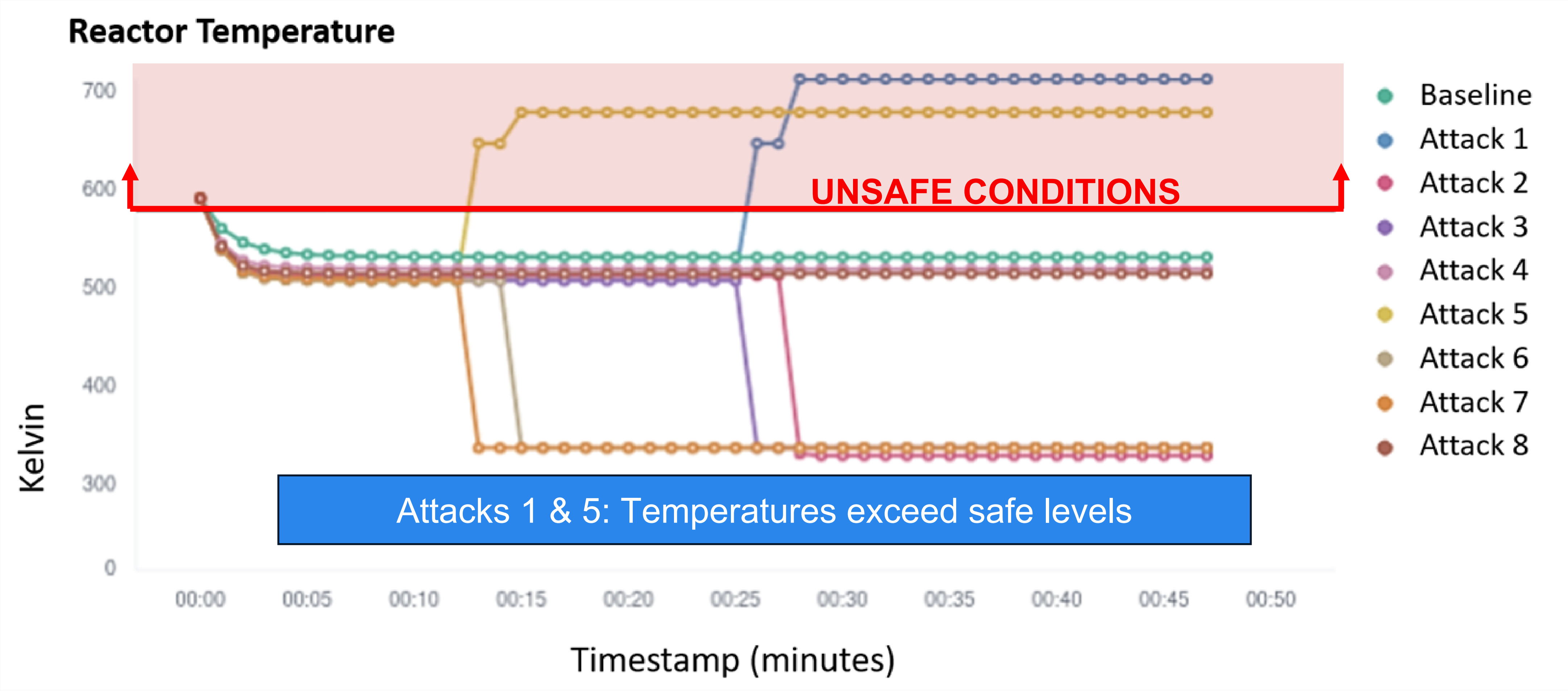
PWR = Pressurized Water Reactor   DNBR = Departure From Nucleate Boiling Ratio   C2 = Command & Control

Top Level Scores

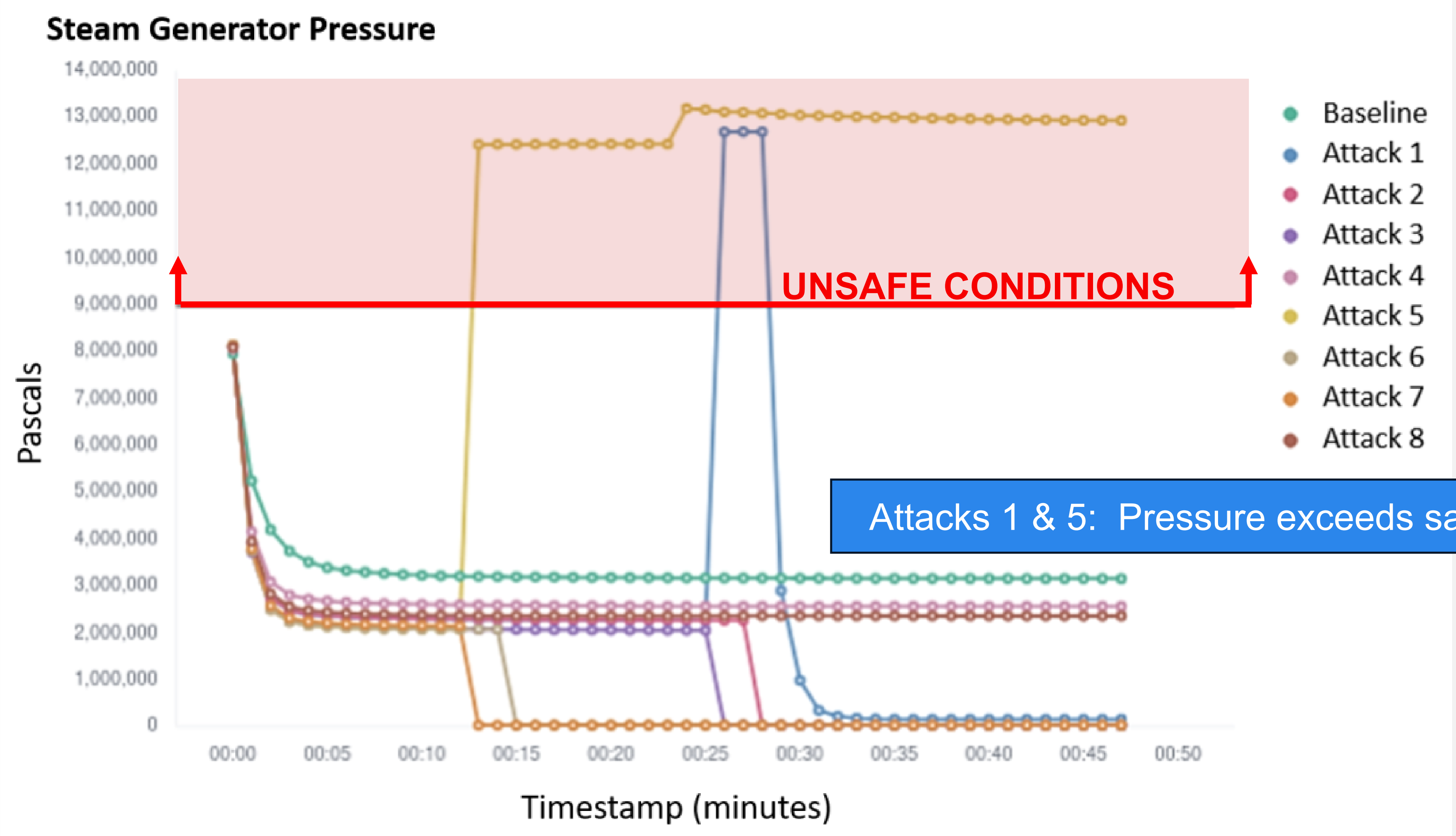


Attacks of Highest Concern: Numbers 1 and 5

Attack Effects: Temperature

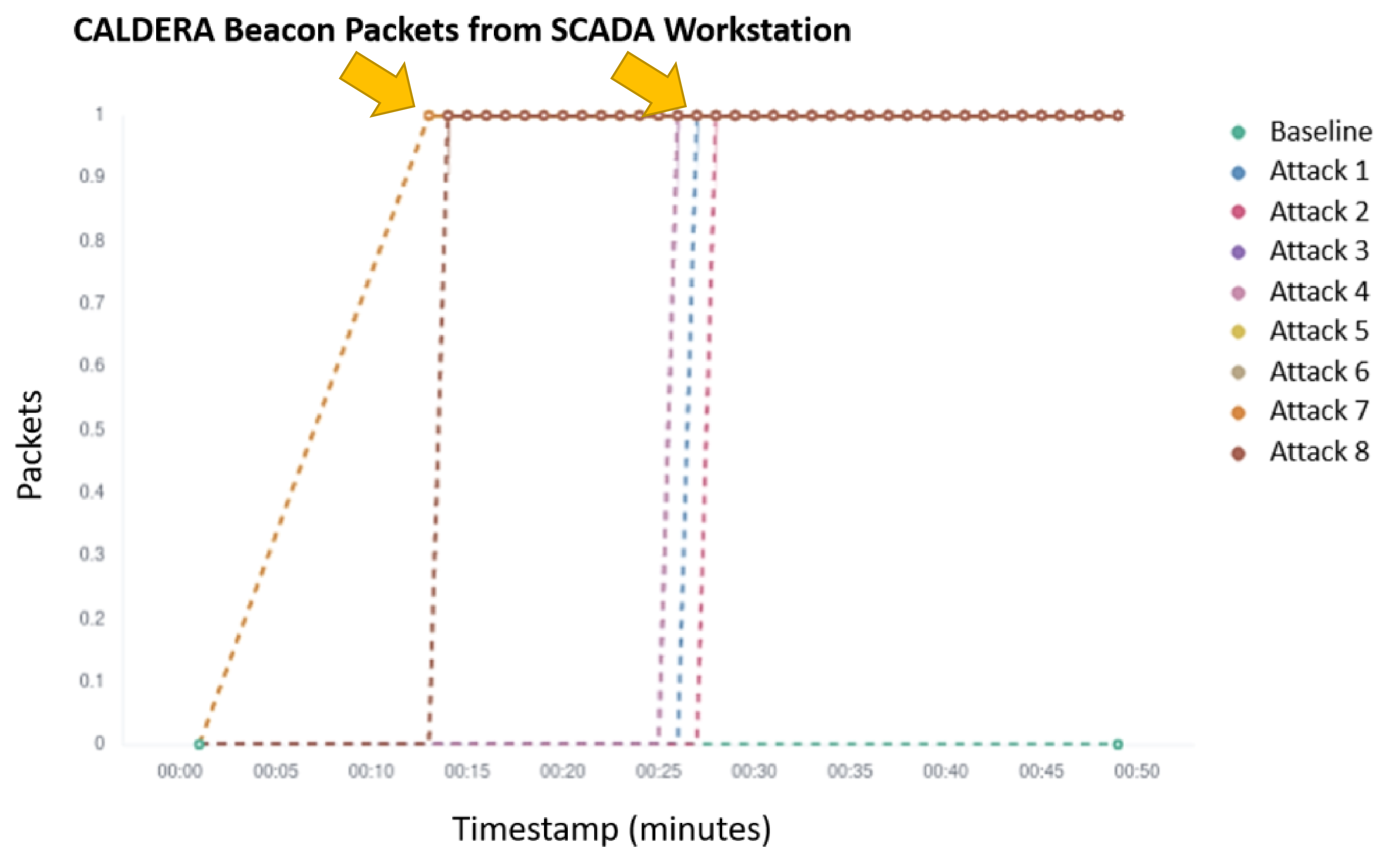


Attack Effects: Pressure



Attacks 1 & 5: Pressure exceeds safe levels

Attack Effects: Speed of Malware

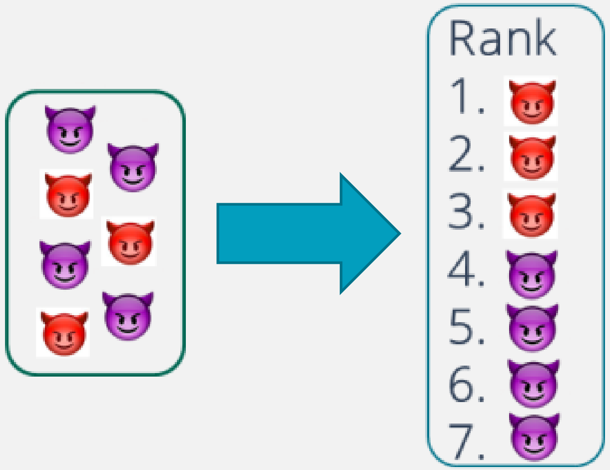


With insider knowledge:
~12 mins to reach target

Without knowledge:
~26 minutes

Conclusion

Cyber resilience is a growing need for ICS



The ADROC platform uses system emulation to

- Model the **system of interest**
- Model the **threats of interest**
- Generate data to quantify the **impact of the threat** on the system
- **Prioritize threats** by their impact to the system mission

Questions?

Jamie Thorpe, jthorpe@sandia.gov