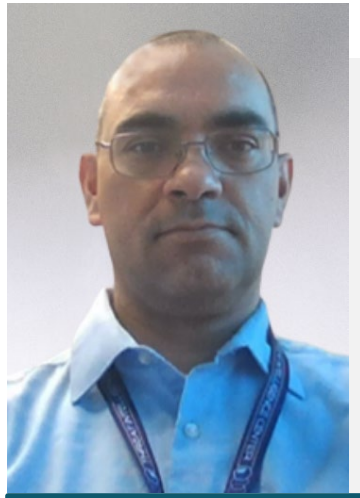


SERC Talks: "How Can We Model Cyber Attacks and Systems to Characterize Resilience of Critical Infrastructure Systems?"

February 23, 2022 | 1:00 PM ET

Dr. Eric Vugrin
Distinguished Member of Technical Staff, Cyber Resilience Research and Development, Sandia National Laboratories

CYBER RESILIENCE

- ❑ Today's session will be recorded.
- ❑ An archive of today's talk will be available at: www.sercuarc.org/serc-talks/ as well as on the SERC YouTube channel.
- ❑ Use the Q&A box to queue up questions, reserving the chat box for comments, and questions will be answered during the last 5-10 minutes of the session.
- ❑ If you are connected via the dial-in information only, please email questions or comments to SERCtalks@stevens.edu.
- ❑ Any issues? Use the chat feature for any technical difficulties or other comments, or email SERCtalks@stevens.edu.

SYSTEMS ENGINEERING RESEARCH CENTER

SERC Talks: "How Can We Model Cyber Attacks and Systems to Characterize Resilience of Critical Infrastructure Systems?"

SERC TALKS

Dr. Eric Vugrin
Distinguished Member of Technical Staff,
Cyber Resilience Research and Development
Sandia National Laboratories

CYBER RESILIENCE

Dr. Peter Beling, SERC Research Council Member; Professor and Associate Director, Intelligent Systems Lab, Hume Center for National Security and Technology, Grado Department of Industrial and Systems Engineering at Virginia Tech

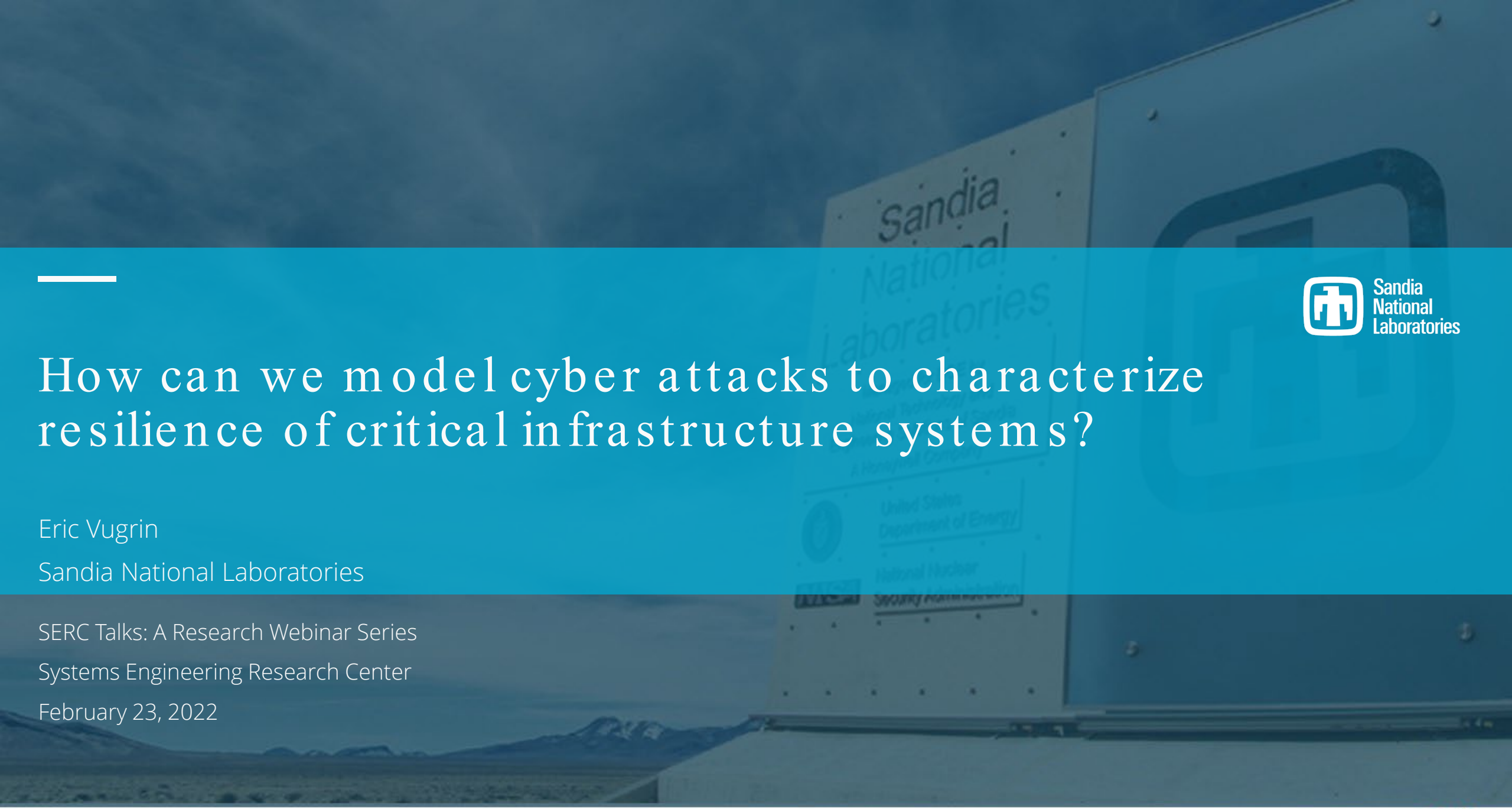
DISCLAIMER

The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense, OUSD (R&E), nor the SERC.

No Warranty. This SERC - Stevens Institute of Technology Material is furnished on an “as-is” basis. SERC and Stevens Institute of Technology makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. SERC and Stevens Institute of Technology does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

This material has been approved for public release and unlimited distribution.



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

Eric Vugrin

Sandia National Laboratories

SERC Talks: A Research Webinar Series

Systems Engineering Research Center

February 23, 2022

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.

SAND2022-1998 PE

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?

This talk describes the Advancing Resilience of industrial Control (ADROC) research effort at Sandia National Laboratories.

Outline

Cyber resilience modeling needs

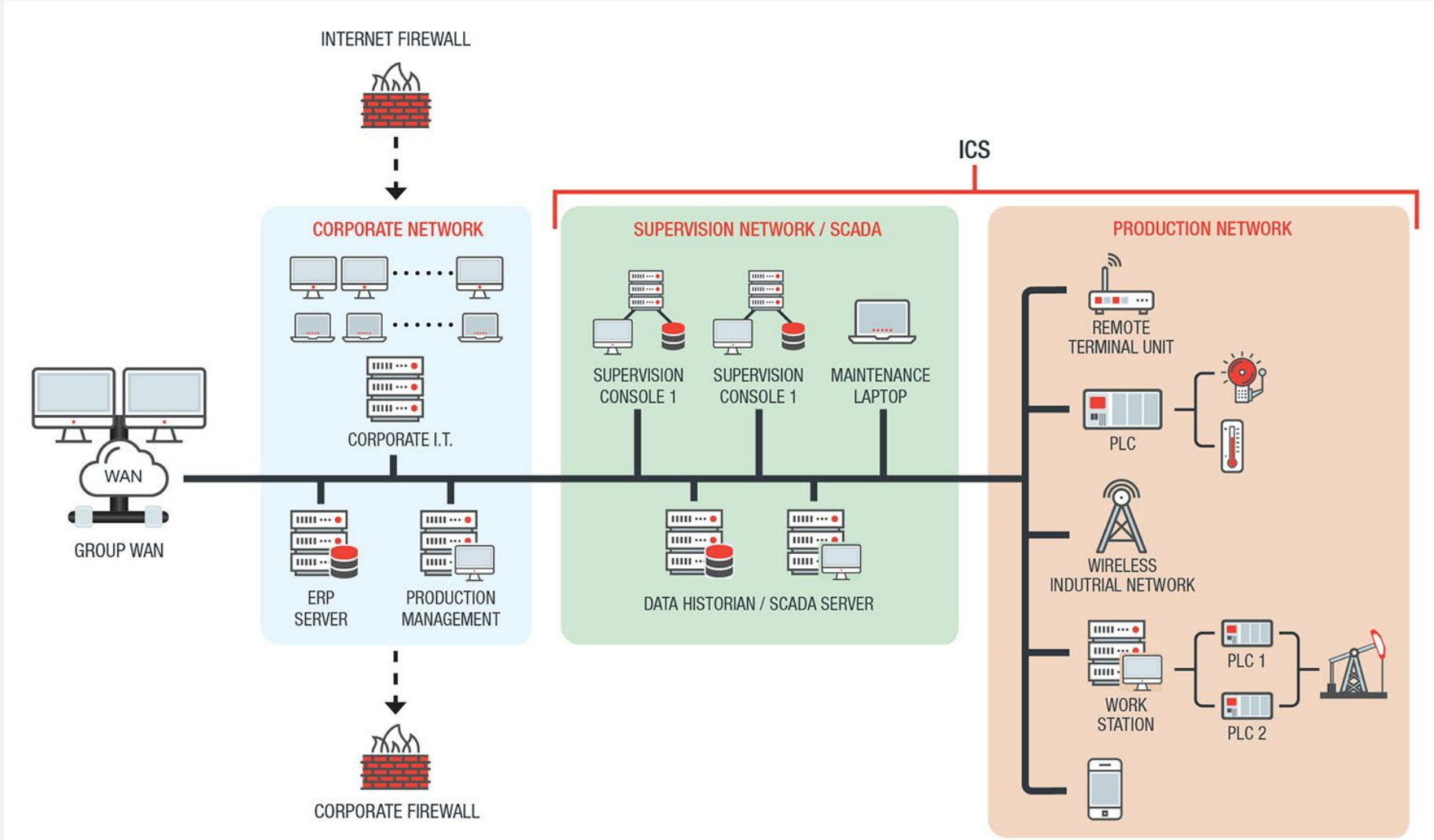
- System
- Threat
- Metrics

An integrated platform

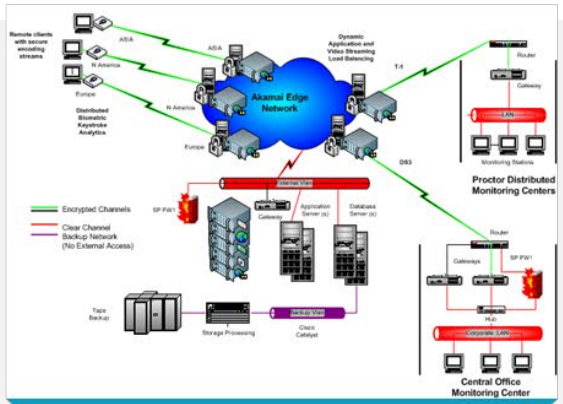
Use case*

* J. Thorpe et al. “A Cyber-Physical Experimentation Platform for Resilience Analysis,” forthcoming the Proceedings of the ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS 2022)

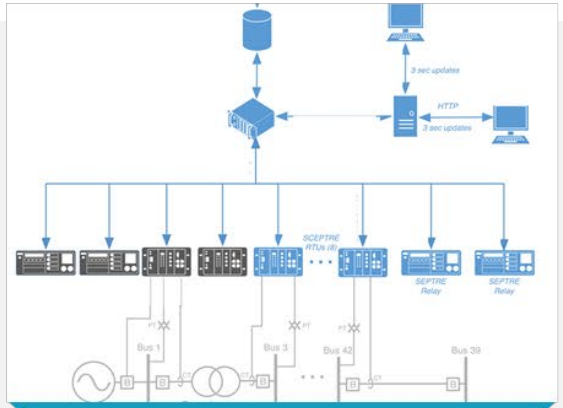
Industrial Control Systems (ICS)



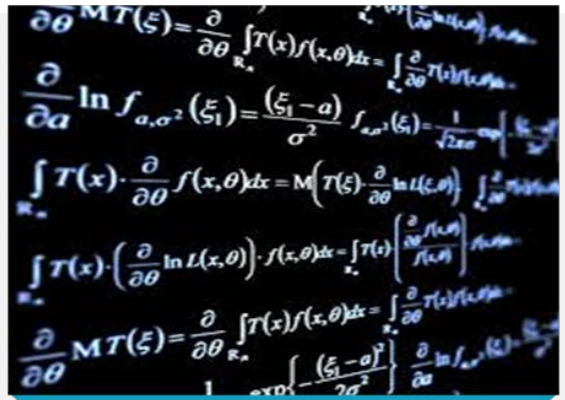
Modeling Cyber Scenarios



ACTUAL SYSTEM



VIRTUALIZED TESTBED



SIMULATION

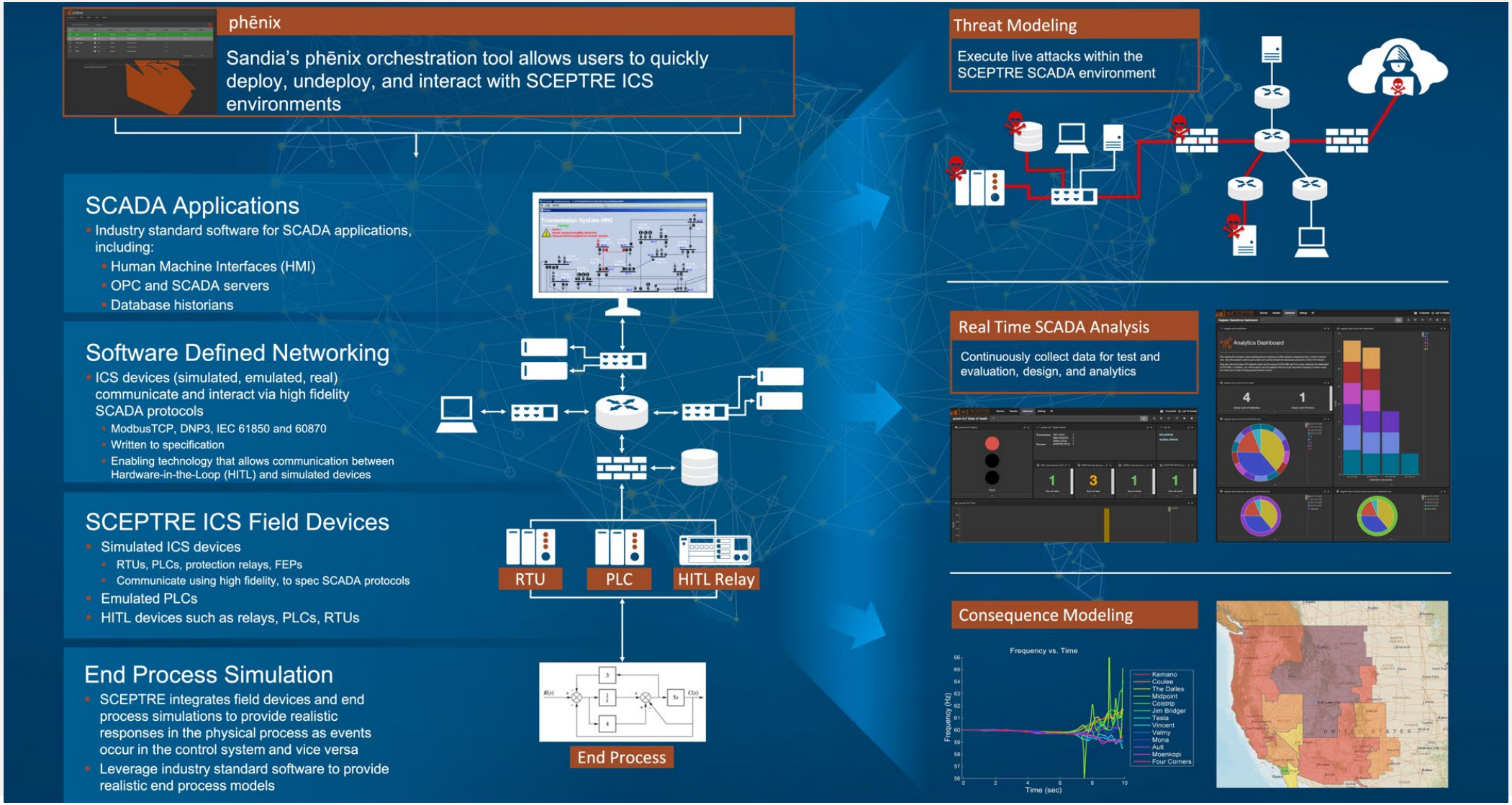
"BAD DAY" BRAINSTORMING

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.

SCEPTRE: Emulation Platform for ICS



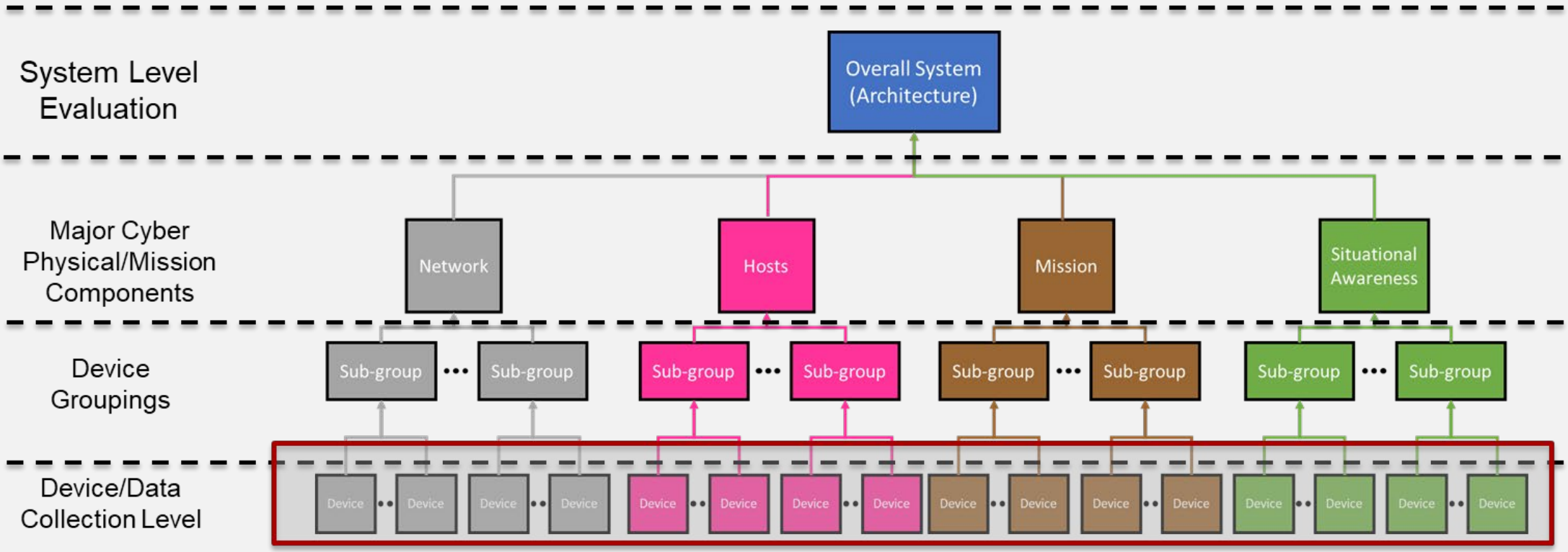
Threat Emulation

Several tools available to provide high fidelity, automated attack platforms

CALDERA is a MITRE-developed threat emulator

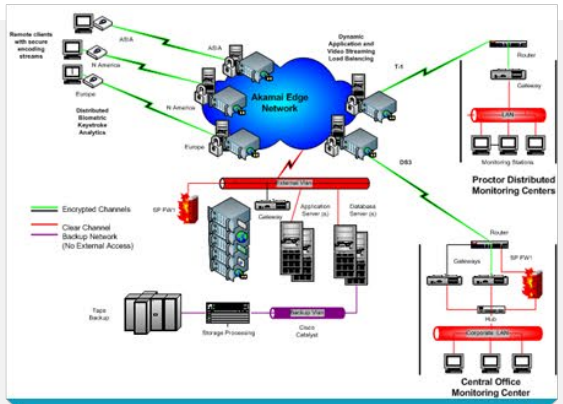
- Attack profile
- Attack goals
- Automated
- Leverages previously observed, real attack tools and techniques
- Closely tied to MITRE ATT&CK framework
- Opportunity to add plug-ins

Resilience Metrics

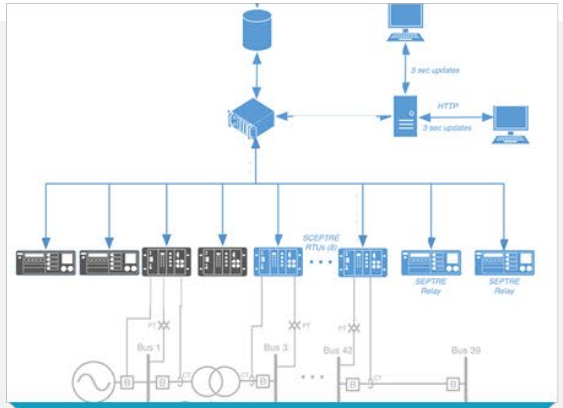


The Resilience VeRification Unit (RevRun) contains an extensible library of resilience metrics for analyzing emulation results.

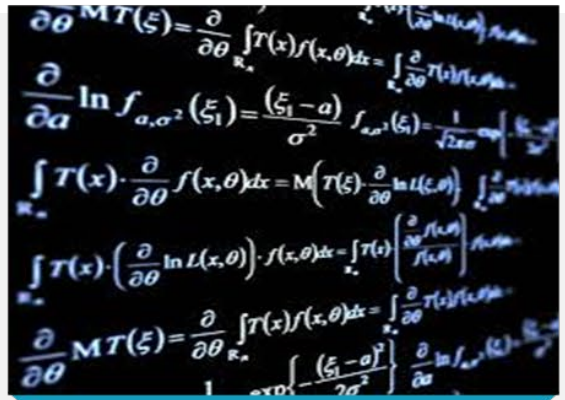
Modeling Cyber Scenarios



ACTUAL SYSTEM



VIRTUALIZED TESTBED



SIMULATION

"BAD DAY" BRAINSTORMING

Increasing Realism
Decreasing Flexibility
Increasing Cost
Increasing Time

Increasing Abstraction
Increasing Flexibility
Decreasing Cost
Decreasing Time

ADROC supplements emulation with mathematical modeling of threats.

ADROC Workflow

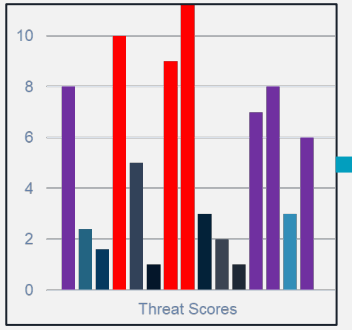
INPUTS: Threats

Parameters

Markov Decision Processes

Data

Outputs: Scores

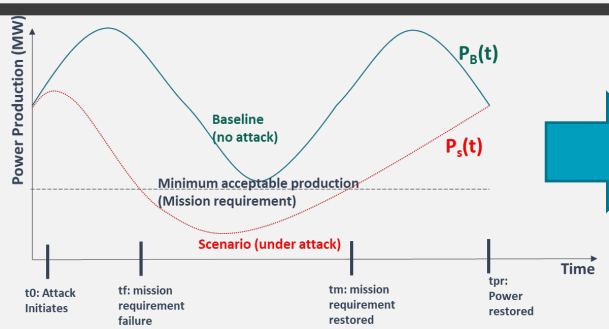


Expt. Control & Metrics: RevRun

Parameters

CALDERA

Effects



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

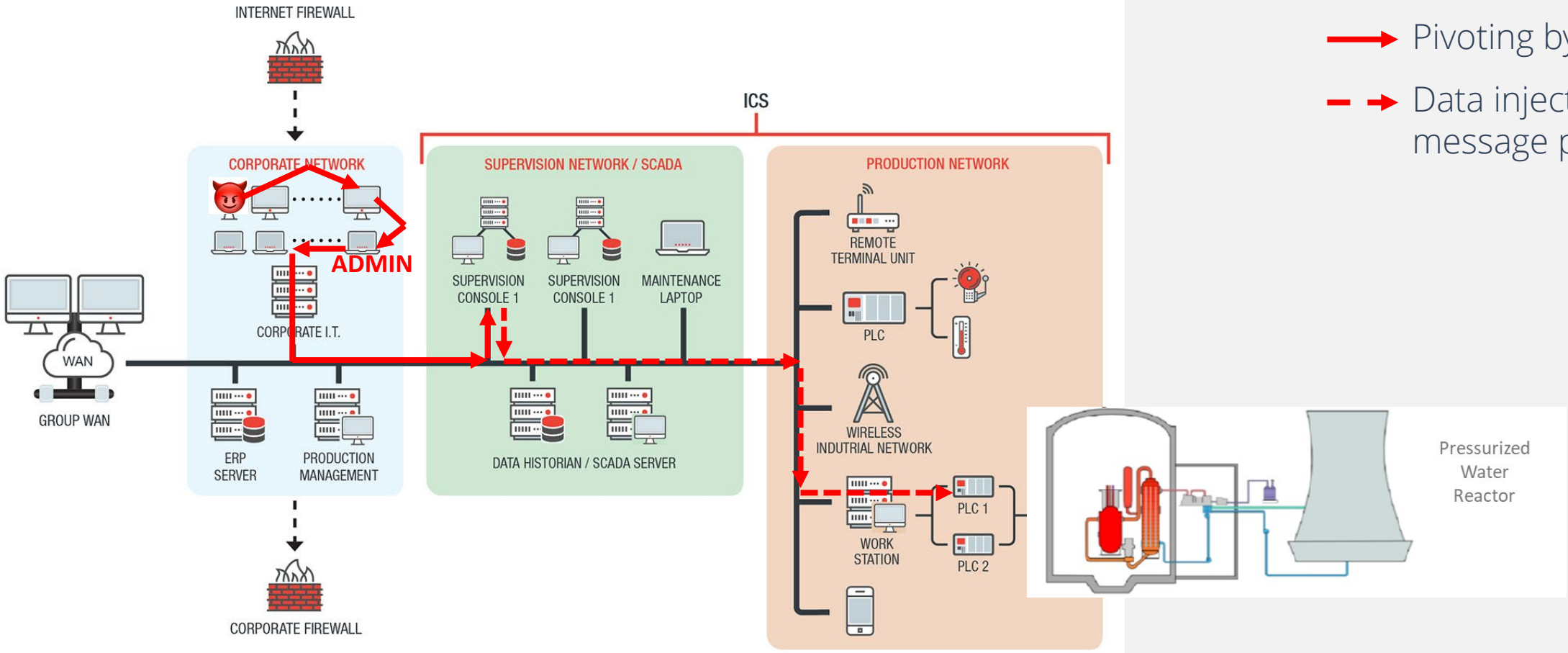
INPUTS:
Priority Threats

Threat Emulators:
CALDERA & ManiPIO

Emulated System:
SCEPTRE

Outputs:
Consequences & Metrics

Example Application: Pressurized Water Reactor



Attacker goal: cause unsafe conditions

Scenarios of Interest*

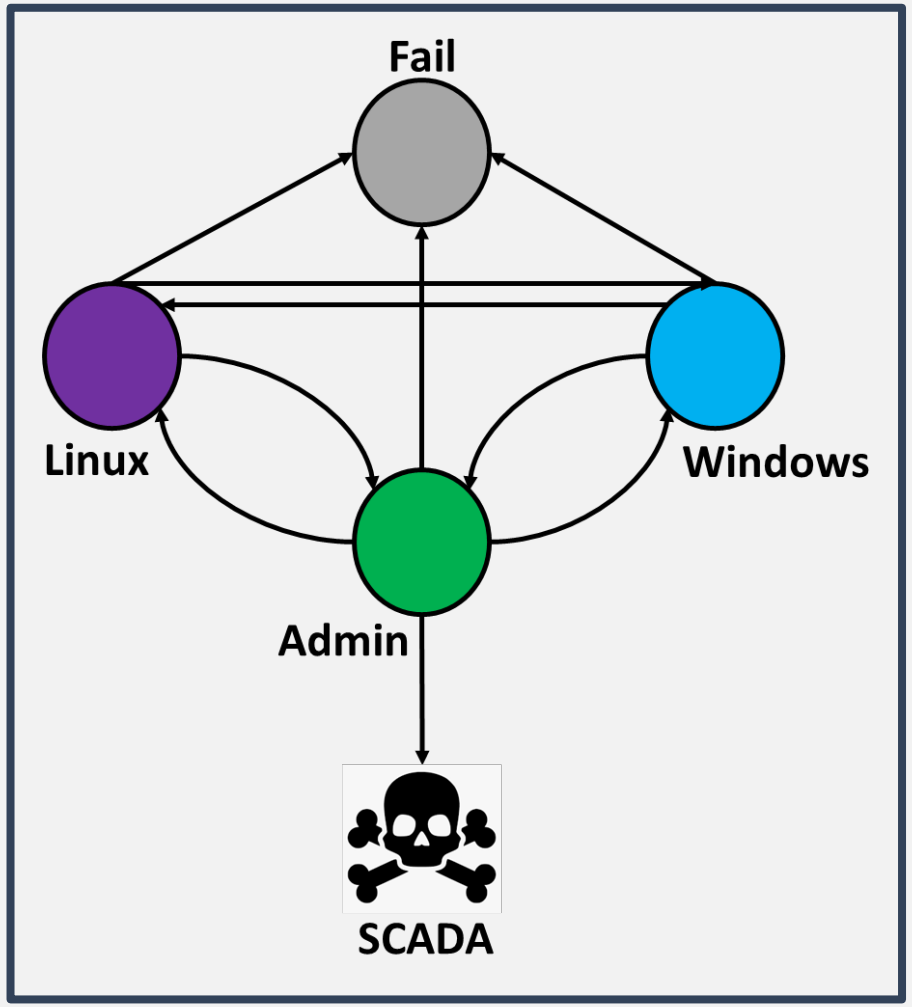
Attack Dimension	Options	Description
Directness?	min path	Attacker had insider knowledge so it pivots to admin machine immediately after initial infection
	full path	No insider knowledge: must perform network discovery & possibly infect multiple machines before getting to admin machine
Malware memory?	Yes	Does not reinfect machines
	No	May reinfect machines
Operating System	Designed to operate on Linux & Windows	Has tools for both operating systems
	Designed for Windows Only	Tools only work on Windows OS machines
Target PLC	Reactor Coolant Pump	Directly affects temperature
	Steam Generator	Directly affects pressure
	Both	Combined effects

Which attacks should we prioritize for investigation?

Can one of the attacks force the PWR to shutdown (e.g., pressure exceeds <9 MPa) ?

* Scenarios are currently notional and intended for illustrative purposes only

Math Model: Malware Variants



Model Structure

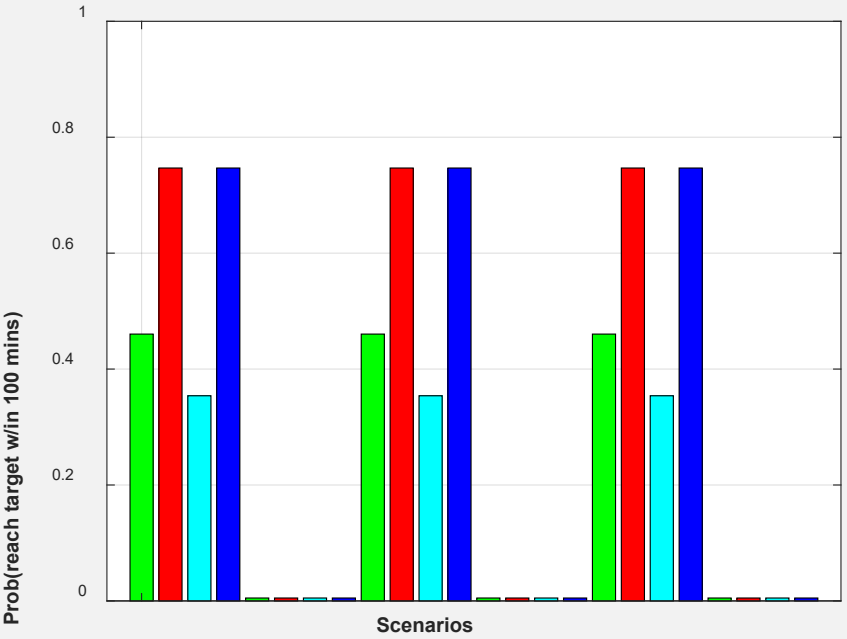
Memory effect on implementation:

- With memory: Doesn't "reinfect" machines (82 states)
- Without memory: reinfects machines (11 states)

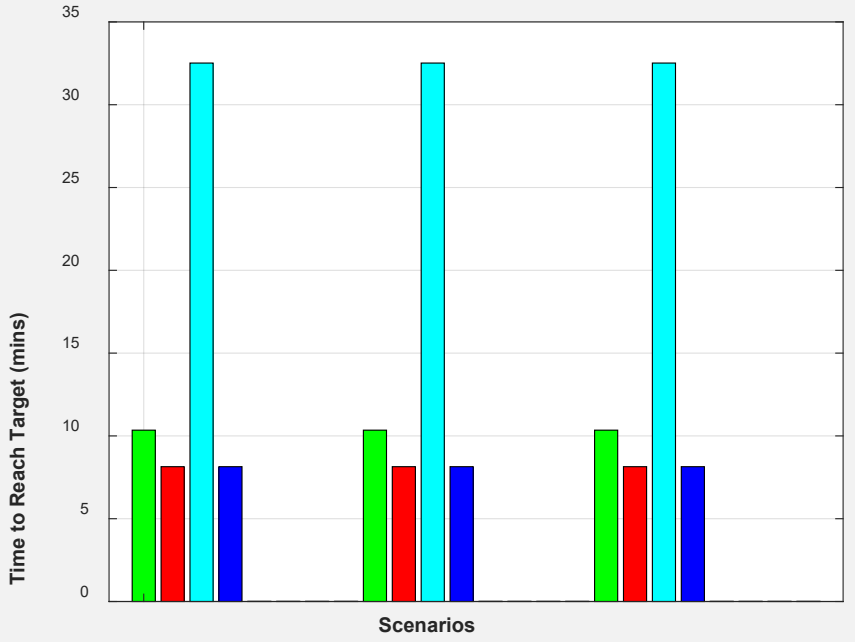
OS target effect on implementation

- Linux: P(success) higher and time required lower for admin machine
- Windows: P(success) and time required higher for admin machine

Math Modeling: Example Results



- Full Path + Memory
- Min Path + Memory
- Full Path + No Memory
- Min Path + No Memory



Limitation: don't know physical impacts of attacks

Further Specifying Attacks

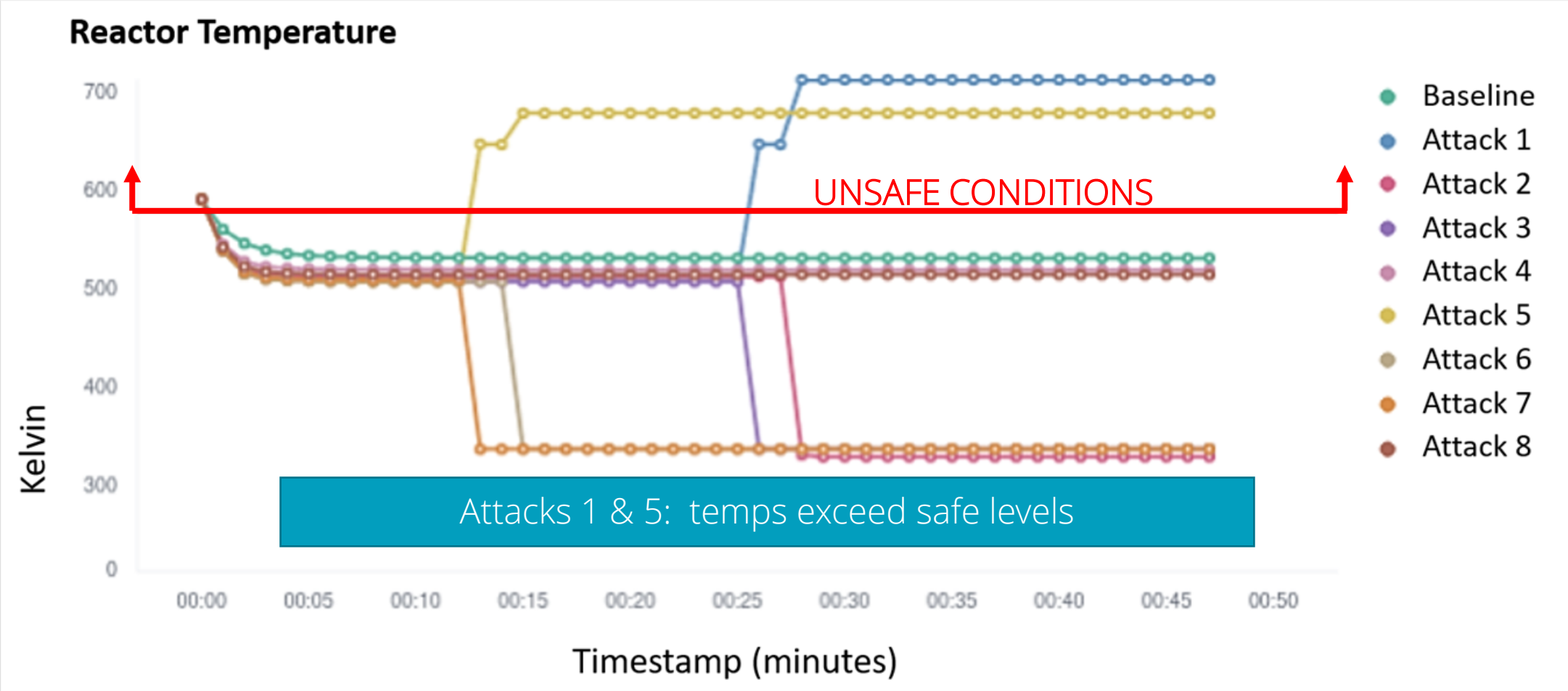
Scenario #	Corporate Network: Attack Path	SCADA Network: Target & Effect
0	N/A	N/A
1	Full path	RCP PLC: set speed to 0 → **overheat core**
2		SG PLC: set valve position to 0→ **increase pressure, overheat core**
3		RCP & SG PLC: change set point in RCP PLC & provide constant sensor reading into SG PLC
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

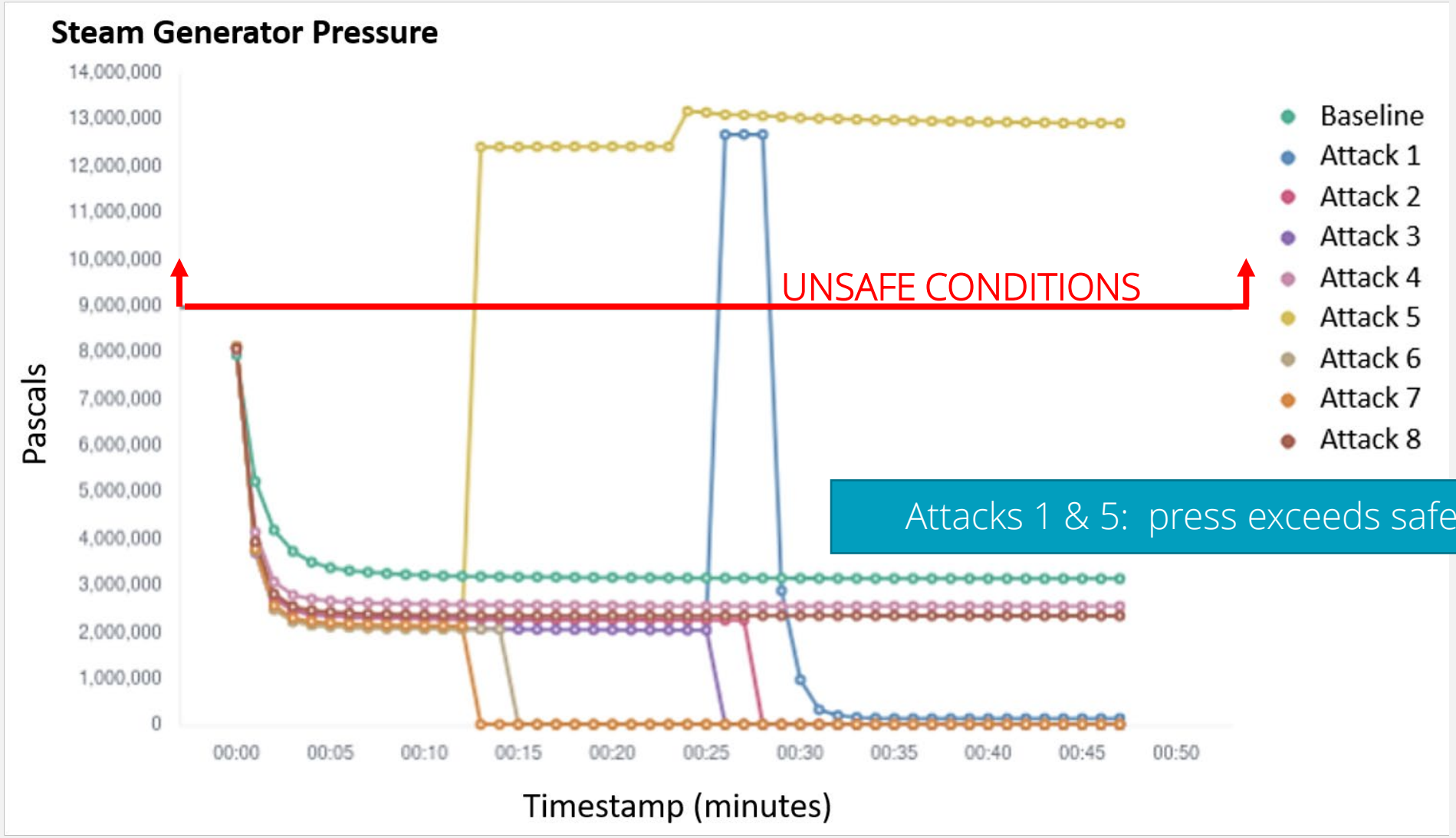
Top Level Scores

Top vs bottom row: effect of insider knowledge
Attacks 1 & 5: reactor coolant pump targeted

Attack Effects: Temperature

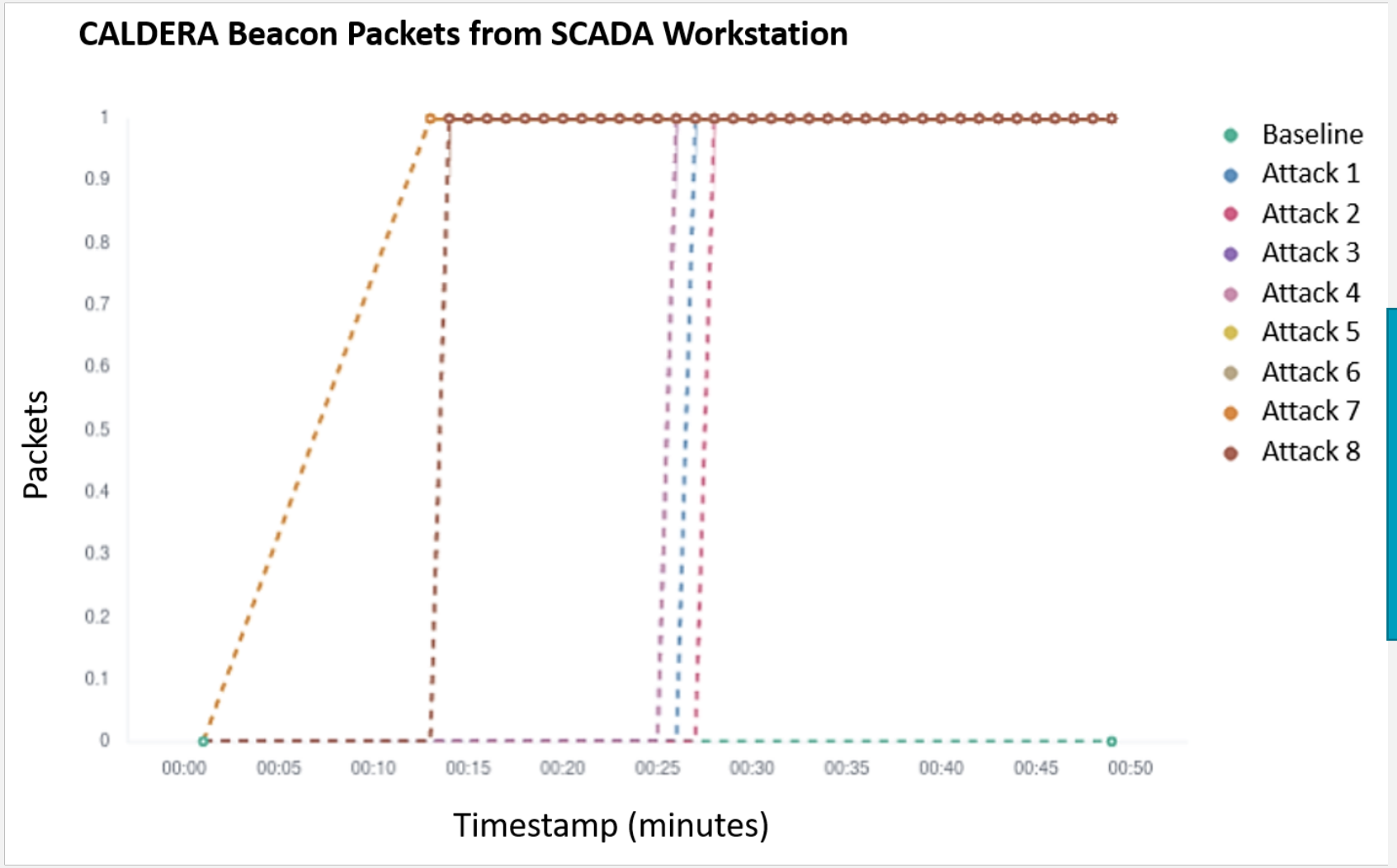


Attack Effects: Pressure



Attacks 1 & 5: press exceeds safe levels

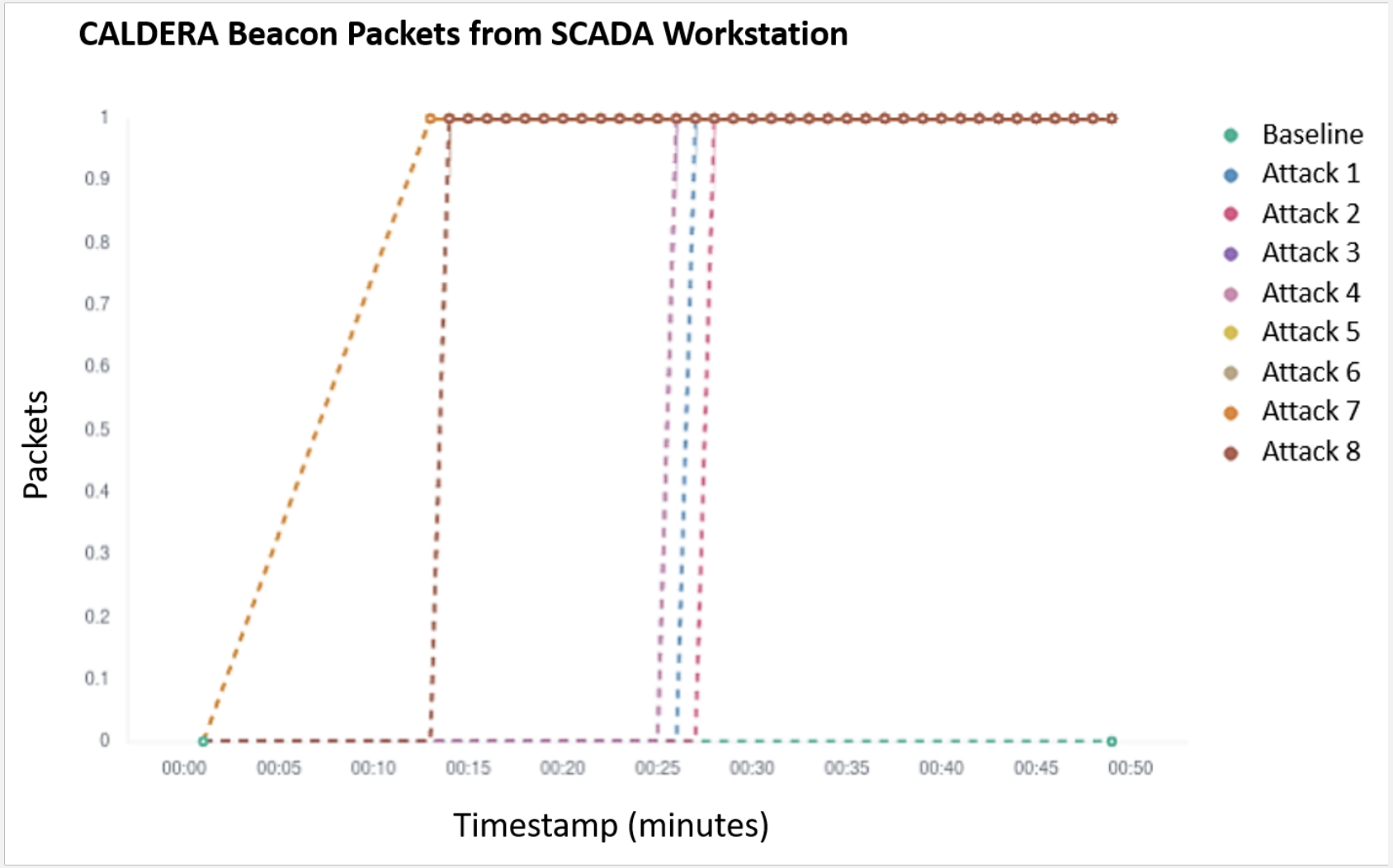
Attack Effects: Speed of Malware



With insider knowledge:
~12 mins to reach target

Without knowledge:
~26 minutes

Attack Effects: Speed of Malware



Data can inform requirement development for mitigations

Summary & Next Steps

Cyber resilience is growing need for ICS

Modeling can provide means for exploring resilience of ICS

The ADROC project employs a hybrid modeling approach

- Mathematical modeling
- Emulation (virtual testbeds)

Future research: leverage reinforcement learning methods to inform mathematical model development

Acknowledgments

ADROC team: Jamie Thorpe, Amanda Gonzales, Chris Mairs, Tim Ortiz, Meghan Sahakian, Eric Vugrin

Nuclear Power Plant and Threat Modeling: Andrew Hahn, Ray Fasano, Tim Ortiz, Chris Lamb

Management support: Craig Lawton, Jen Depoy, Derek Hart, Lon Dawson

The ADROC project is funded by Sandia's Resilient Energy Systems Mission Campaign.

QUESTIONS AND DISCUSSION

UPCOMING TALK

SERC TALKS

"Cyber Resilience: a Technical Concept or Vague Desiderata?"

Dr. Alexander Kott, Chief Scientist, U.S. Army Research Laboratory; Army Senior Research Scientist (ST) for Cyber Resilience, U.S. Army

Wednesday, April 6, 2022 at 1PM ET | REGISTRATION OPEN

"Cyber Resilience" Series Moderator:

Dr. Peter Beling, SERC Research Council member, Virginia Tech

CONTACT

Webinar Coordinator: Ms. Mimi Marcus, Stevens Institute of Technology – mmarcus@stevens.edu

For more information, visit the SERC Talks page.

SERC TALKS

SYSTEMS ENGINEERING RESEARCH CENTER

THANK YOU FOR JOINING US!

Please check back on the SERC website for today's recording and future SERC Talks information.

www.sercuarc.org/contact-us/