SAND2023-05354C

Sandia National Laboratories

Exceptional service in the national interest

Using the Information Harm Triangle to Model Sequences of Unsafe Control Actions in I&C Systems

Lee T. Maccarone, Andrew S. Hahn, Michael T. Rowland

ICONE30; 21-26 May 2023; Kyoto, Japan

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 and wholly owned subsidiary of Honeywell International Inc. for the U.S. onal Nuclear Security Administration under contract DE-NA0003525.

Why use the Information Harm Triangle (IHT)?

- The IHT combines Systems-Theoretic Process Analysis (STPA) with cybersecurity analysis
  - STPA maps unsafe control actions (UCAs) to system losses

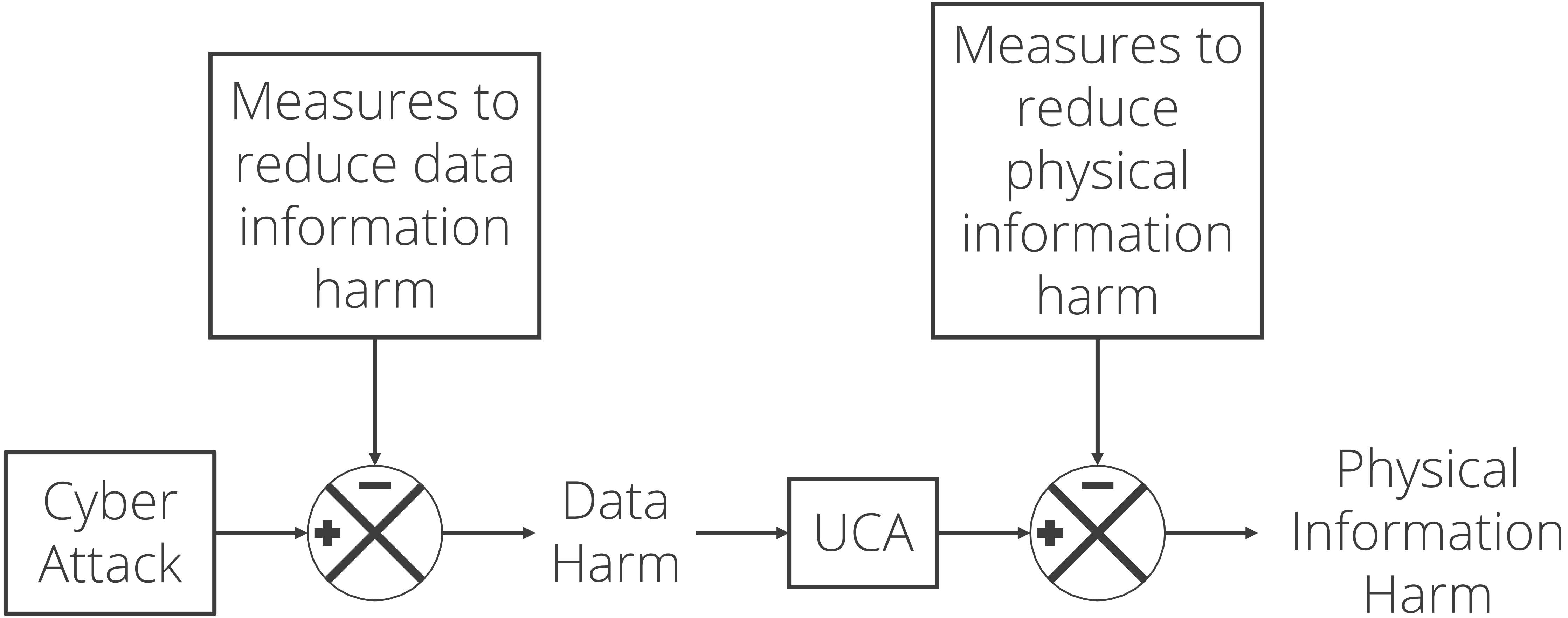
- Integrity and availability are prioritized when analyzing the cybersecurity of industrial control systems

- We need to understand how an adversary's actions in the digital domain cause consequences in the physical world

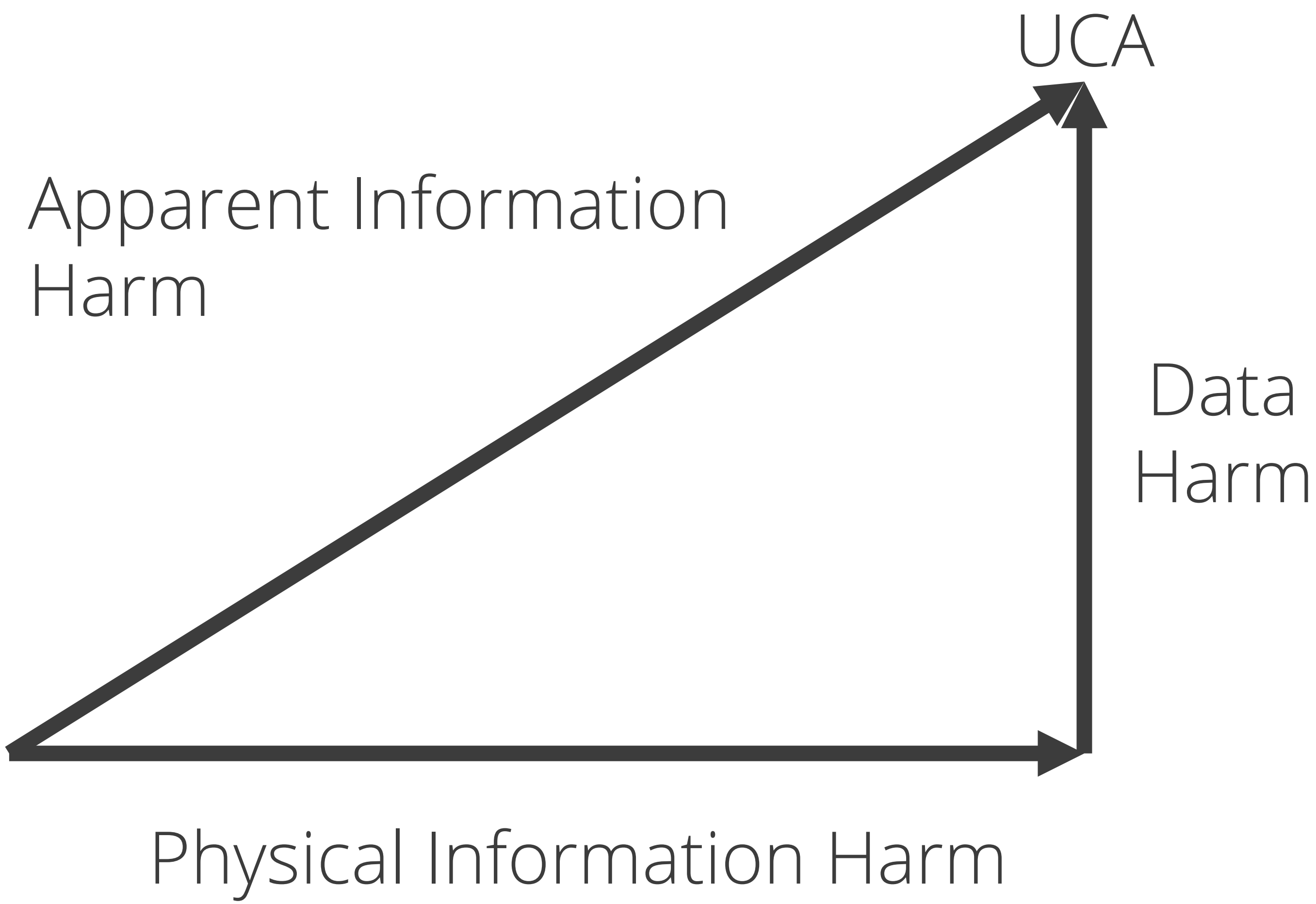
- We can act in both the digital space and physical space to limit the impact of a cyber-adversary to the OT system

What is the IHT?

Cyber attacks cause physical harm through UCAs


Measures to reduce data information harm
Measures to reduce physical information harm
Cyber Attack
+
−
Data Harm
UCA
+
−
Physical Information Harm

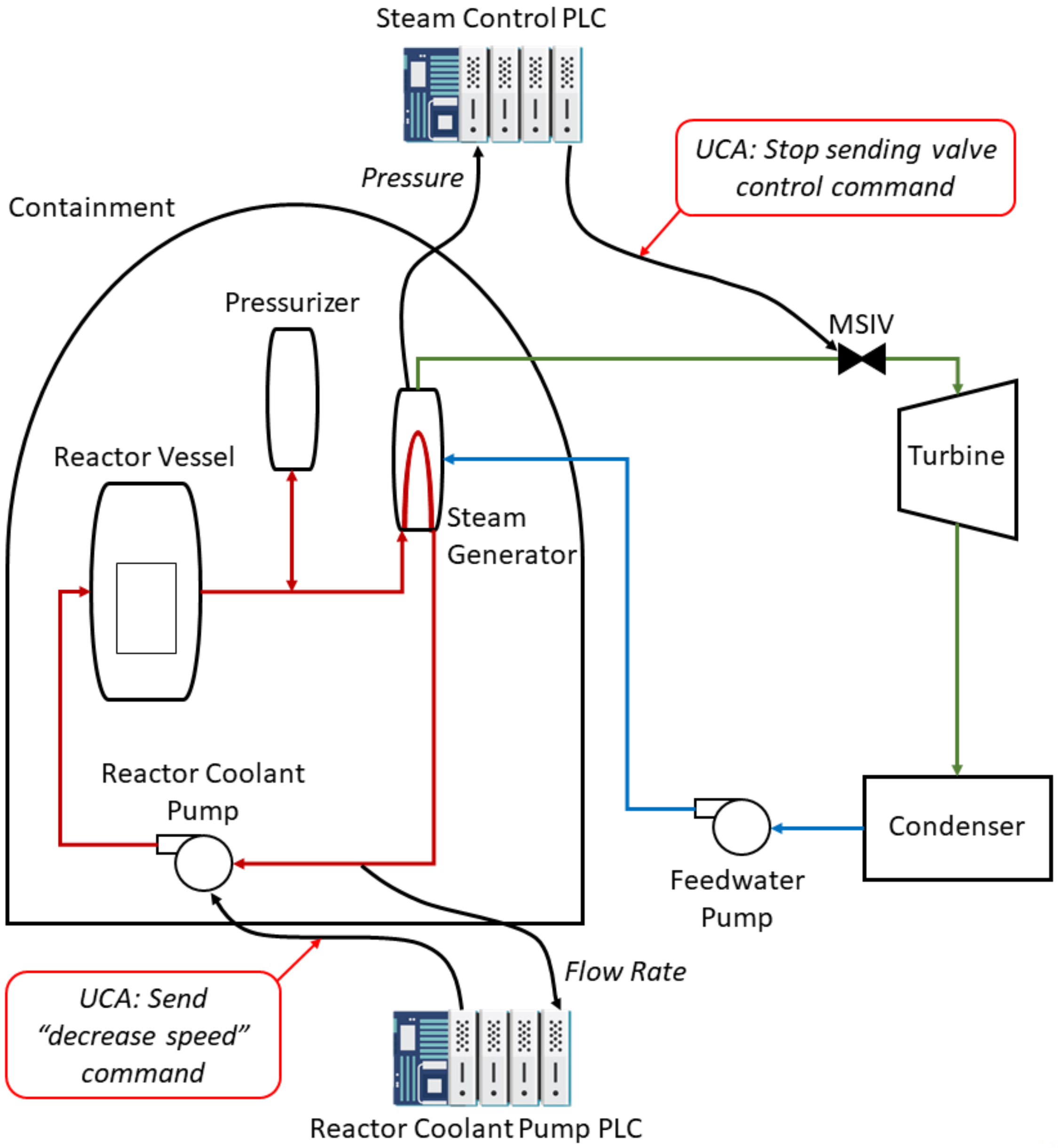
The IHT combines data harm and physical information harm into a single figure



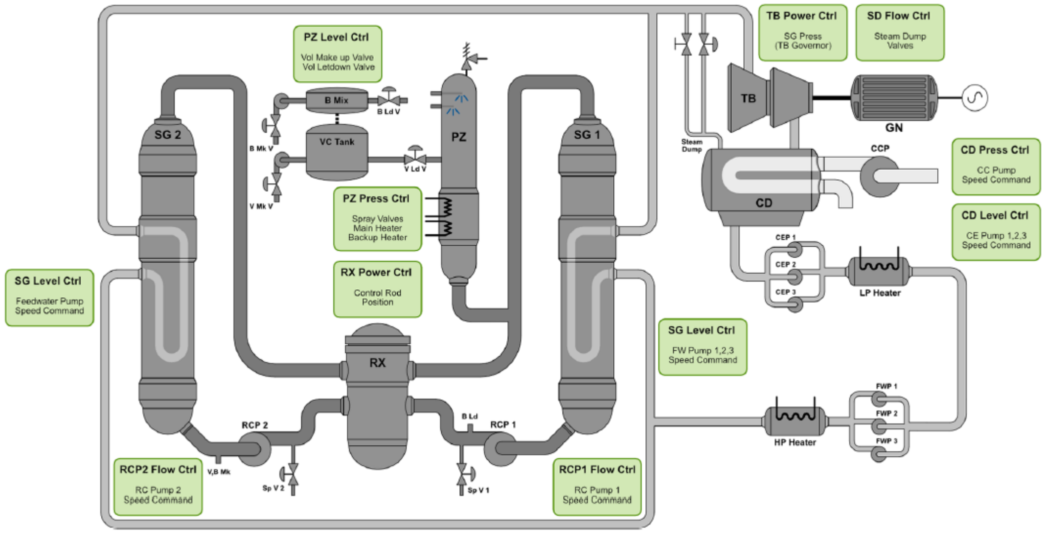
Can the IHT be used to analyze multiple UCAs?

Experimental Scenario

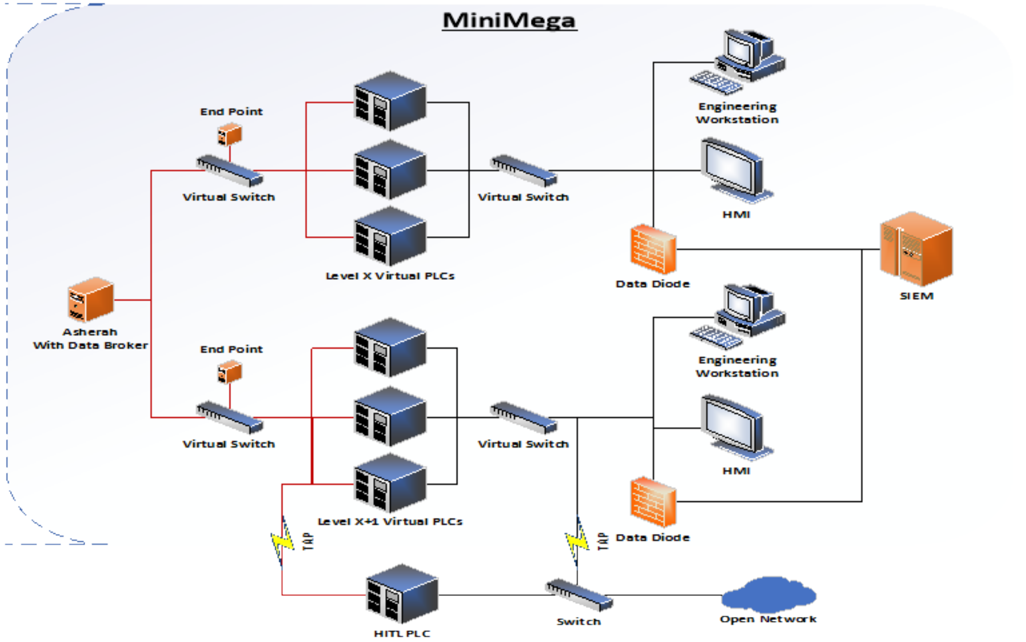
- The steam generator pressure and reactor coolant pump controllers were evaluated using STPA to identify UCAs
- Two UCAs were identified to combine in a dynamic scenario:
  - UCA 1: Send reactor coolant pump decrease speed command
  - UCA 2: Freeze steam generator throttle position during transient
- Time between initiation of these UCAs was varied to evaluate their impact to physics



Modeling and simulation were used to study the combination of UCAs



+



Process Model
(Asherah Nuclear Power Plant Simulator)

Network Emulation
(MiniMega)

Citation: Silva RB, Shirvan K, Piqueira JR, Marques RP. Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment. International Conference on Nuclear Security (ICONS), 10-14 Feb 2020 in Vienna Austria 2020.

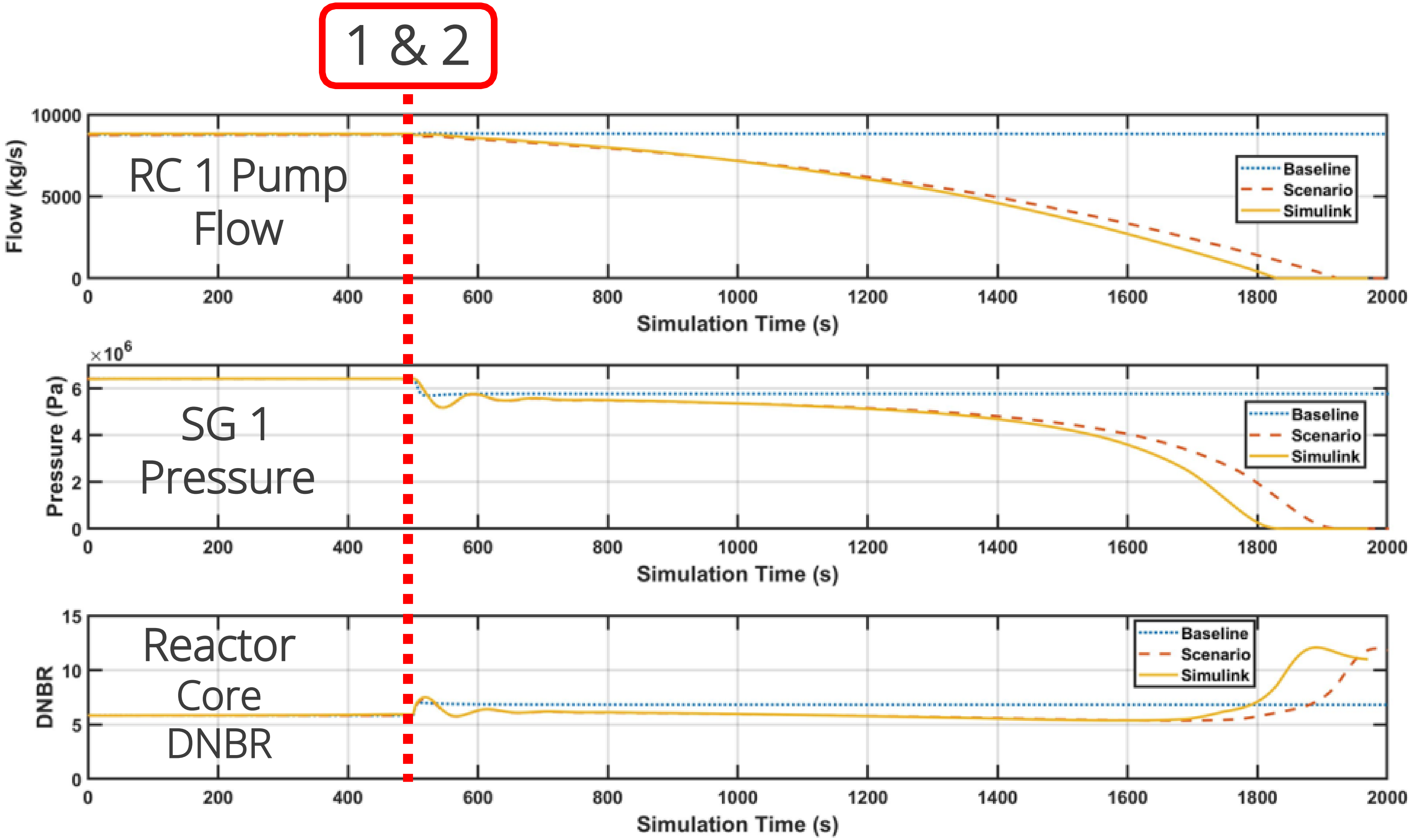
Simulations show the simultaneous UCA combination causes a gradual decrease in steam generator pressure

UCA 1:

- Initiated at 500 seconds
- Sets input value to PID controller to 11,000 kg/s (desired setpoint ~8800 kg/s)
- Causes PID controller to decrease the pump flow rate

UCA 2:

- Initiated at 500 seconds
- Sets output value to turbine steam isolation as the previous value (i.e. constant value)
- Causes the actuation value to hold a fixed position initiating rapid depressurization



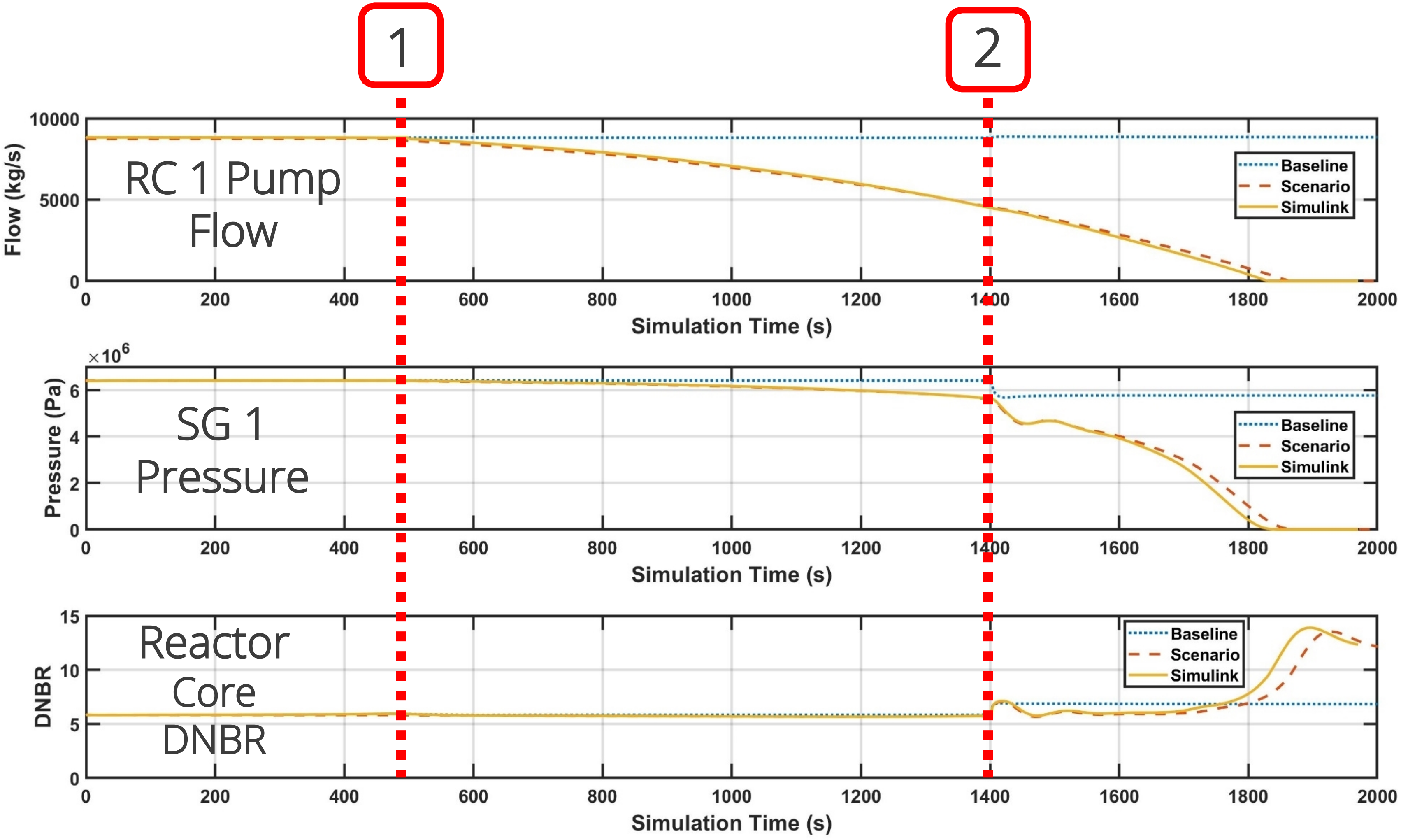
Simulations show the sequential UCA combination causes a sudden decrease in steam generator pressure

UCA 1:

- Initiated at 500 seconds
- Sets input value to PID controller to 11,000 kg/s (desired setpoint ~8800 kg/s)
- Causes PID controller to decrease the pump flow rate

UCA 2:

- Initiated at 1,400 seconds
- Sets output value to turbine steam isolation as the previous value (i.e. constant value)
- Causes the actuation value to hold a fixed position initiating rapid depressurization

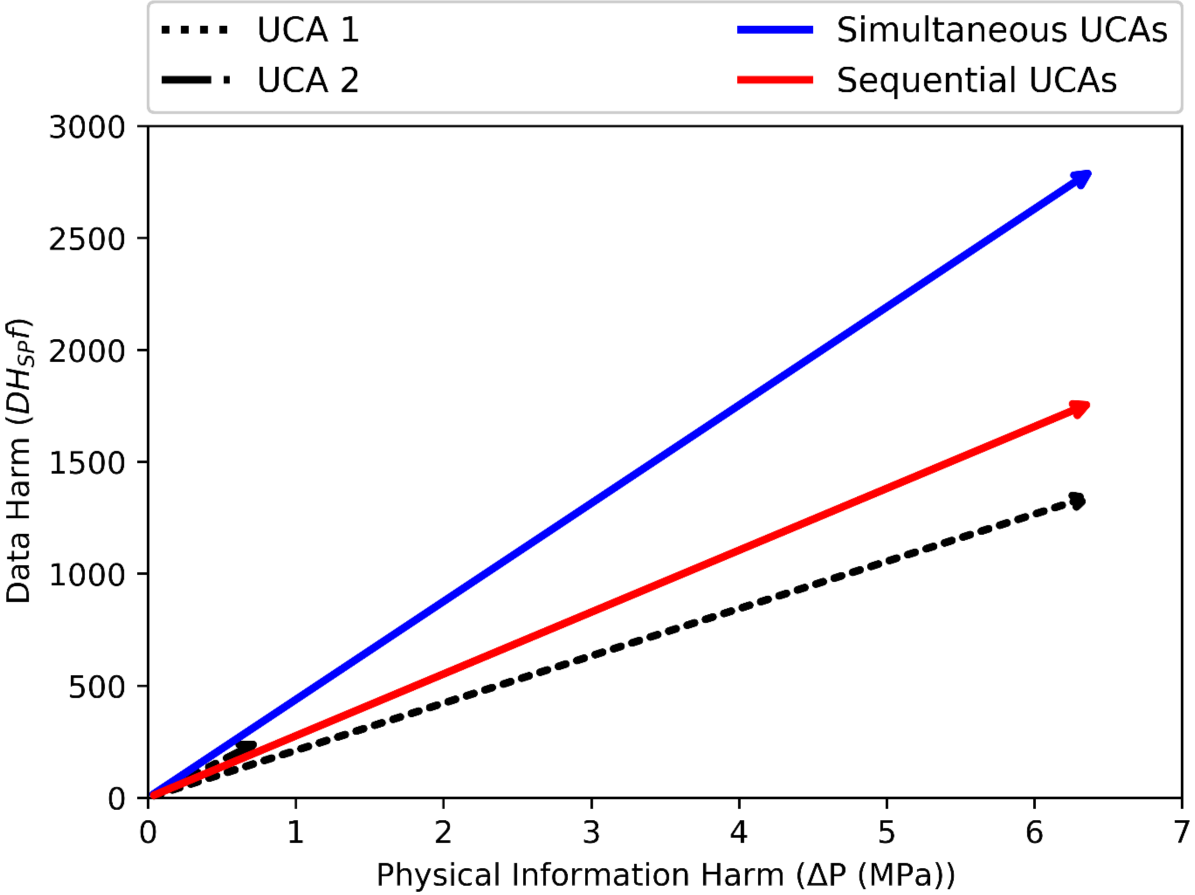


How do we define harm?

- Physical Information Harm:
  - $PIH = P_{nominal} - P_{steady\ state}$

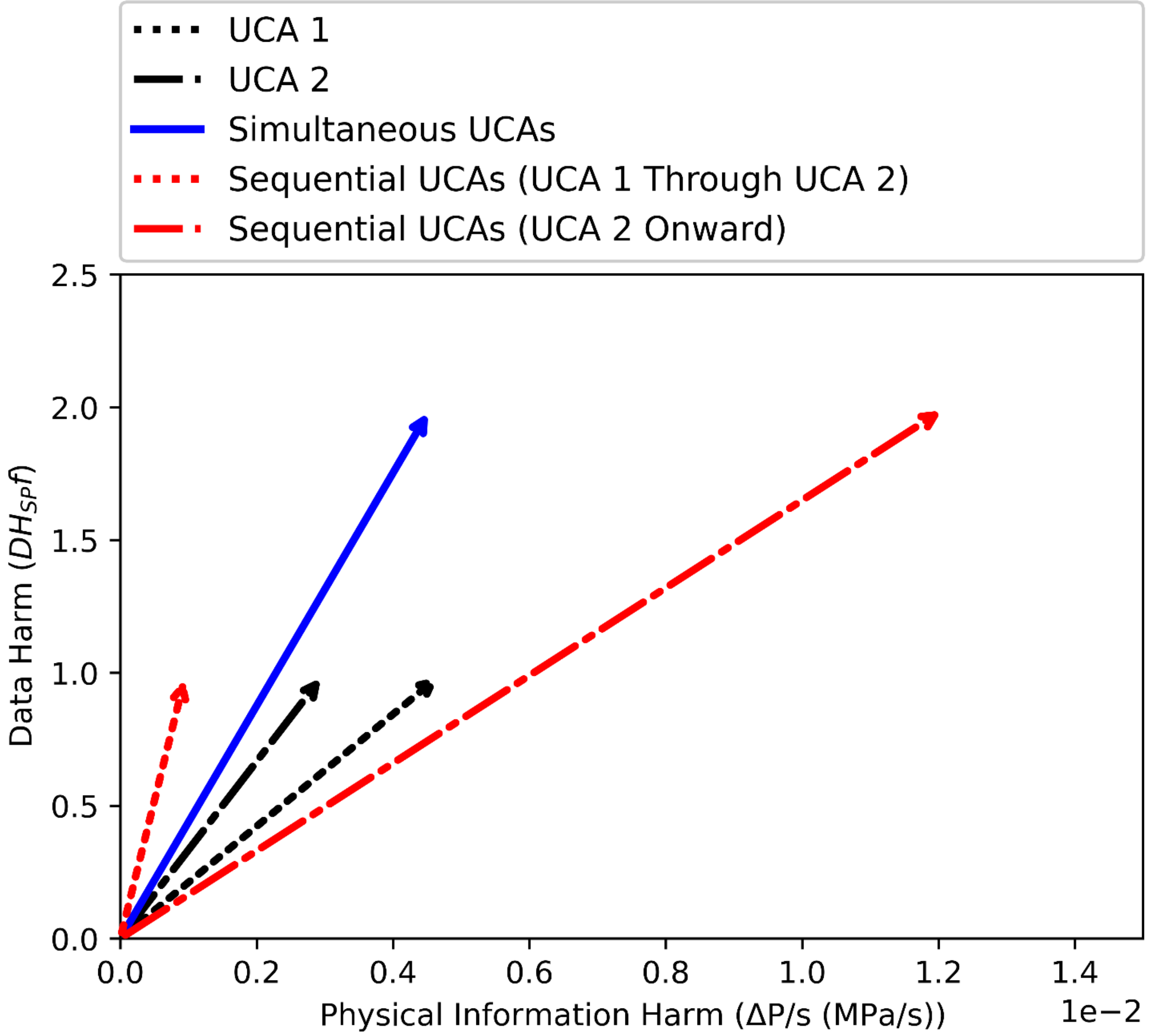
- Data Harm:
  - $DH = DH_{SP} f \Delta t$
  - DH_{SP}: data harm to change a setpoint
  - f: frequency of the PLC
  - Δt: attack duration

IHTs were created to show the total data harm and physical harm



The combinations of UCAs caused the same total physical harm as UCA 1, but required greater data harm

IHTs were created to show the rates of data harm and physical harm



Concluding Remarks

1. The IHT is a new approach for simplifying the design of defense-in-depth security measures for ICSs

2. The IHT combines safety and cybersecurity analyses to inform the selection of security measures

3. The IHT can be used to analyze combinations of UCAs

4. Advanced modeling and simulation tools can be used to validate the IHT and other cybersecurity analysis methods

Thank you for your time and attention

Contact Information:
Lee Maccarone
lmaccar@sandia.gov