Sandia National Laboratories

Exceptional service in the national interest

Using the Information Harm Triangle to Secure OT Systems

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

S4x23, 13-16 February 2023, Miami, FL

SAND2023-12059C

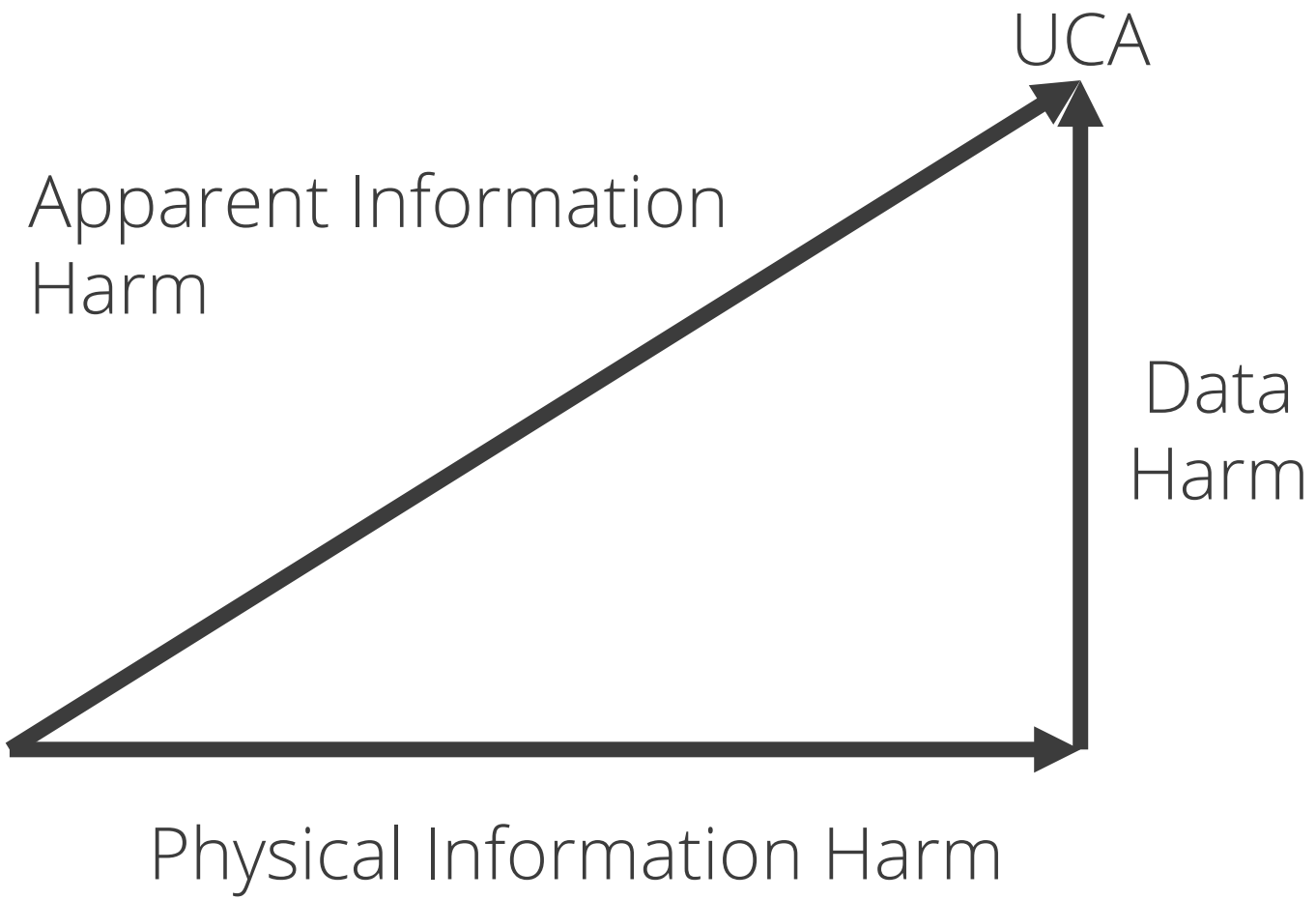
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and wholly owned subsidiary of Honeywell International Inc. for the U.S. onal Nuclear Security Administration under contract DE-NA0003525.

Why use the Information Harm Triangle (IHT)?

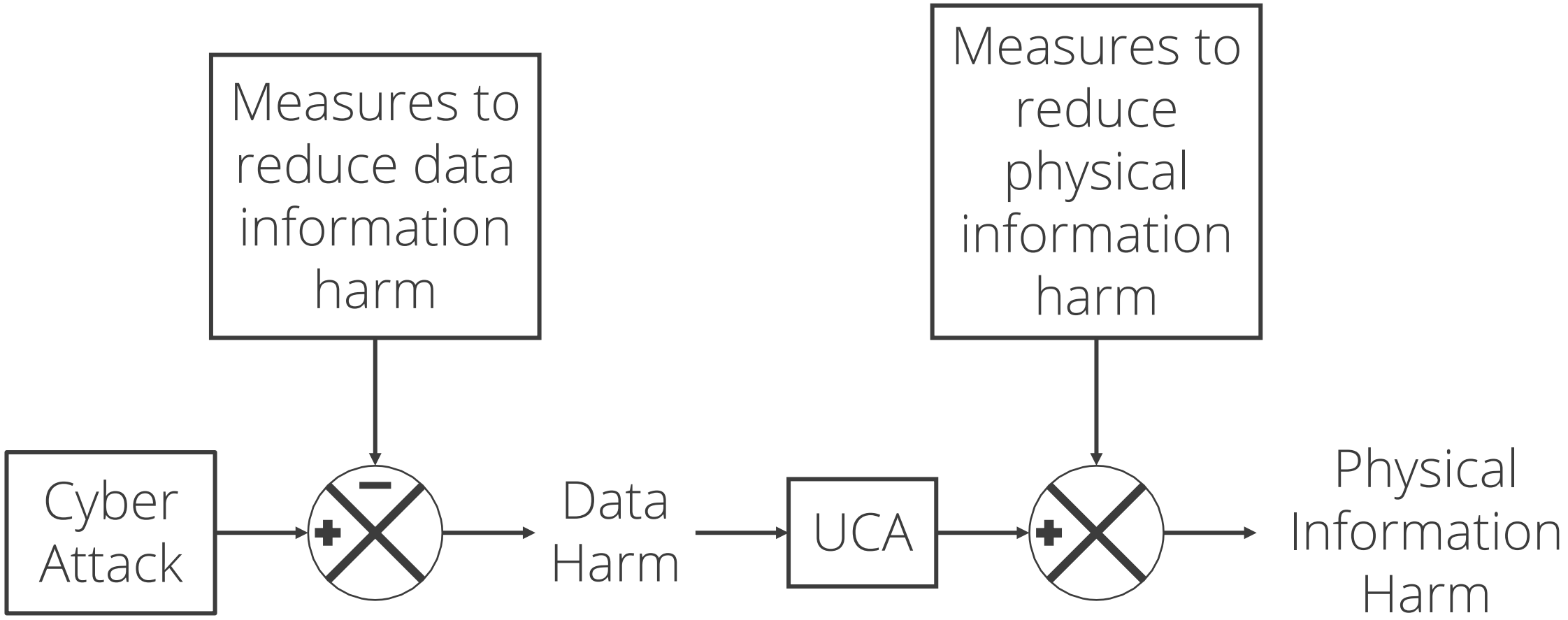
- The IHT combines Systems-Theoretic Process Analysis (STPA) with cybersecurity analysis
  - STPA maps unsafe control actions (UCAs) to system losses
- Integrity and availability are prioritized when analyzing the cybersecurity of OT systems
- We need to understand how an adversary's actions in the digital 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?

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

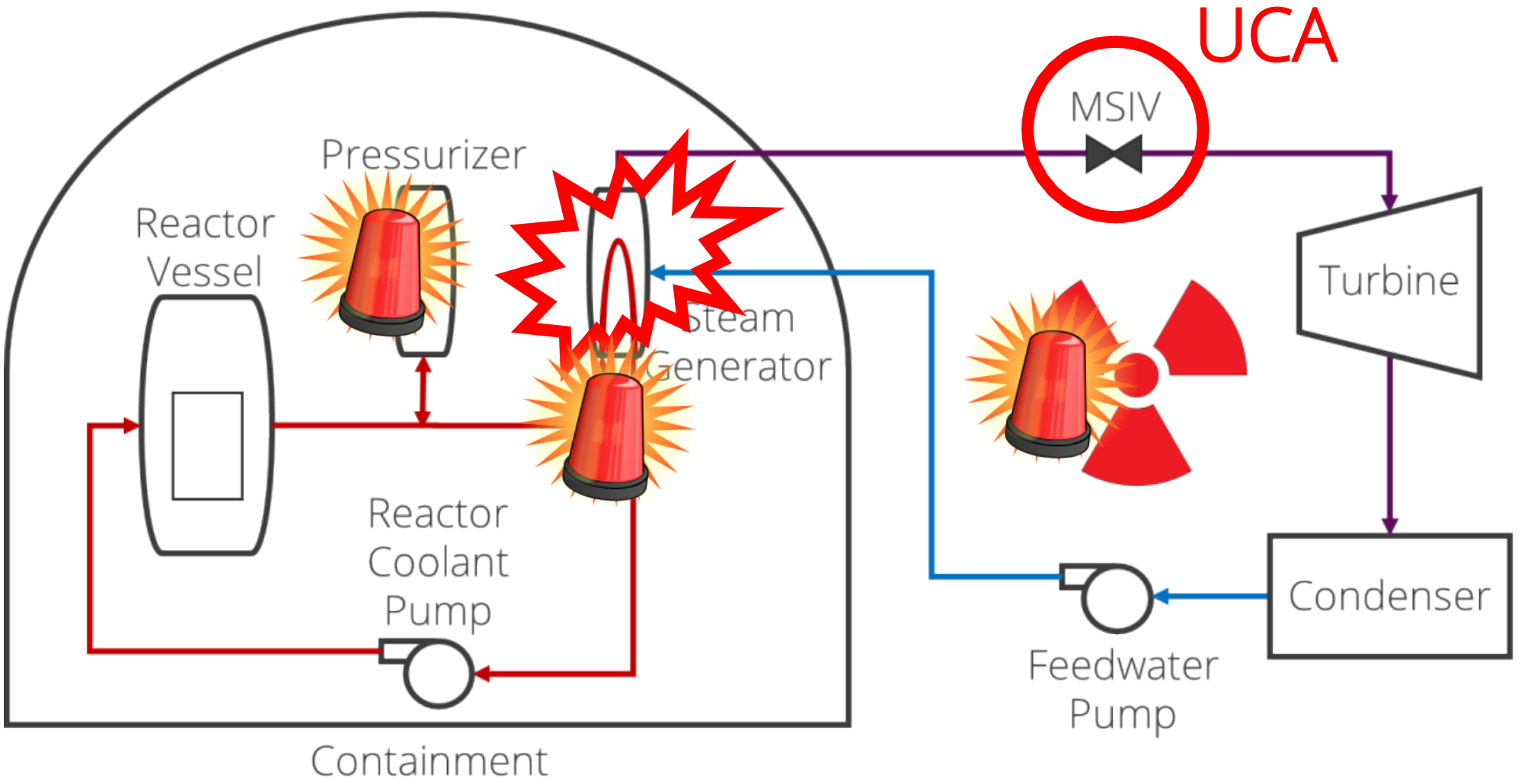


Cyber attacks cause physical harm through UCAs



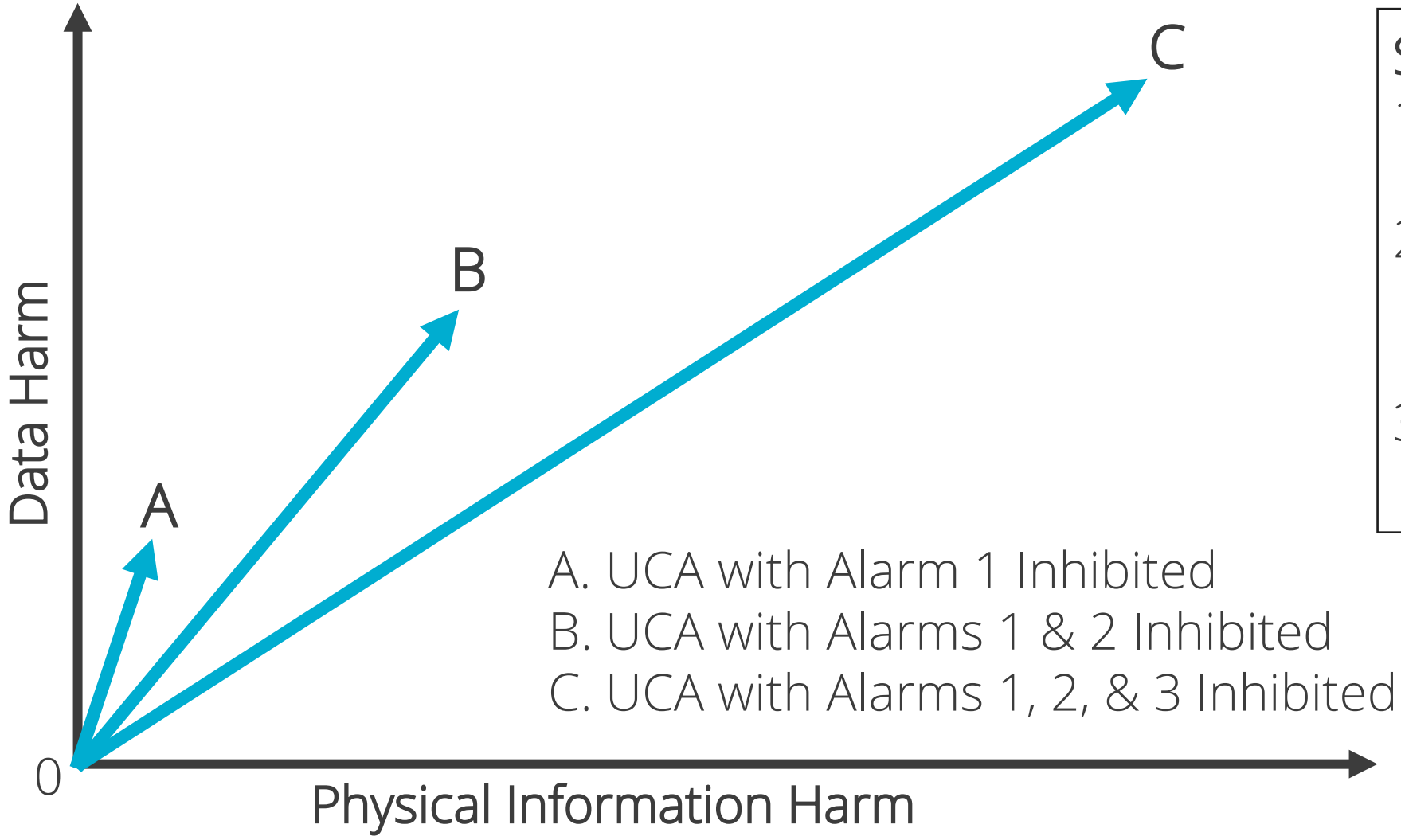
How is the IHT applied?

The main steam isolation valve (MSIV) isolates the steam generator from the secondary system



UCA: Signal to close MSIV is too late after steam generator tube rupture

Data harm is proportional to the number of spoofed indicators, but physical information harm is not

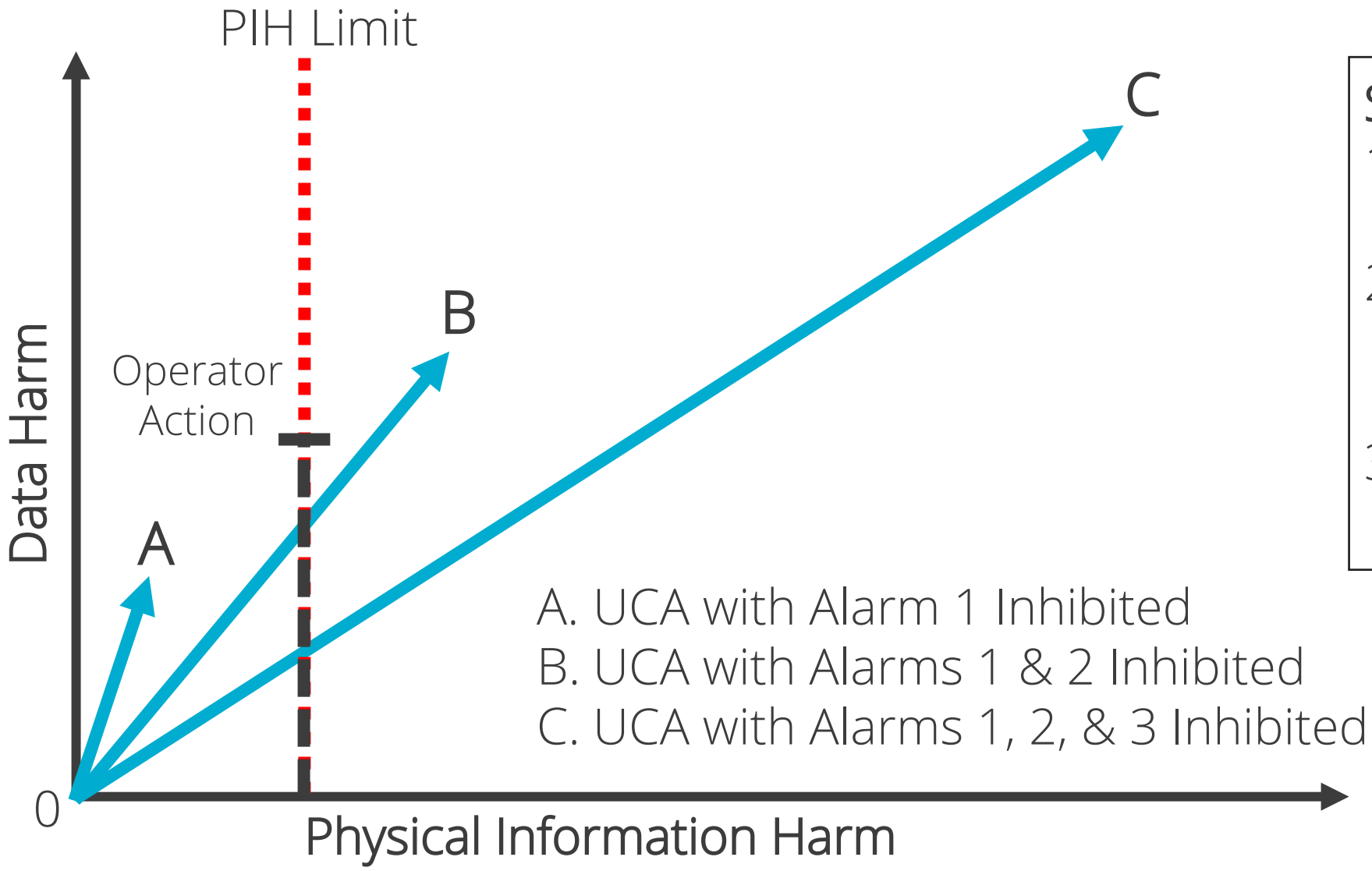


A. UCA with Alarm 1 Inhibited
B. UCA with Alarms 1 & 2 Inhibited
C. UCA with Alarms 1, 2, & 3 Inhibited

SGTR-Related Alarms:

1. Radiation in secondary system
2. Steam generator flow rate mismatch
3. Pressurizer pressure decrease

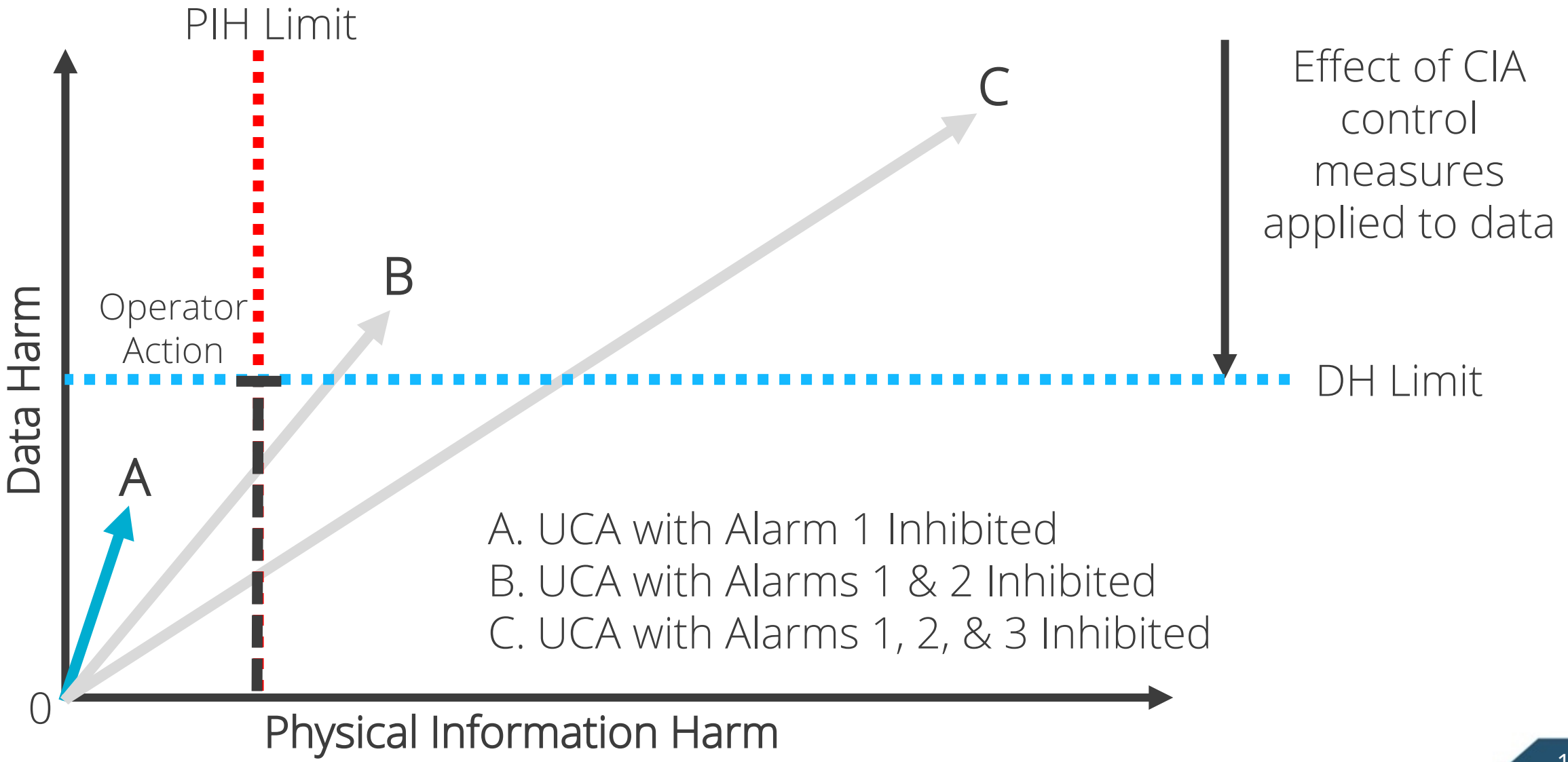
Regulatory limit on radioactivity of secondary coolant is used to define the physical information harm limit



SGTR-Related Alarms:

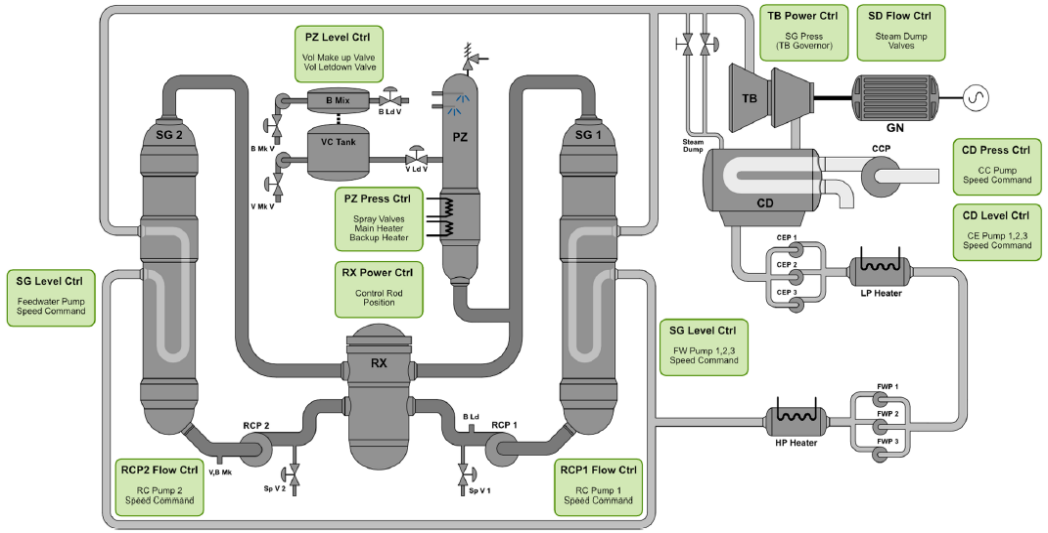
1. Radiation in secondary system
2. Steam generator flow rate mismatch
3. Pressurizer pressure decrease

Data harm measures are used to limit physical harm

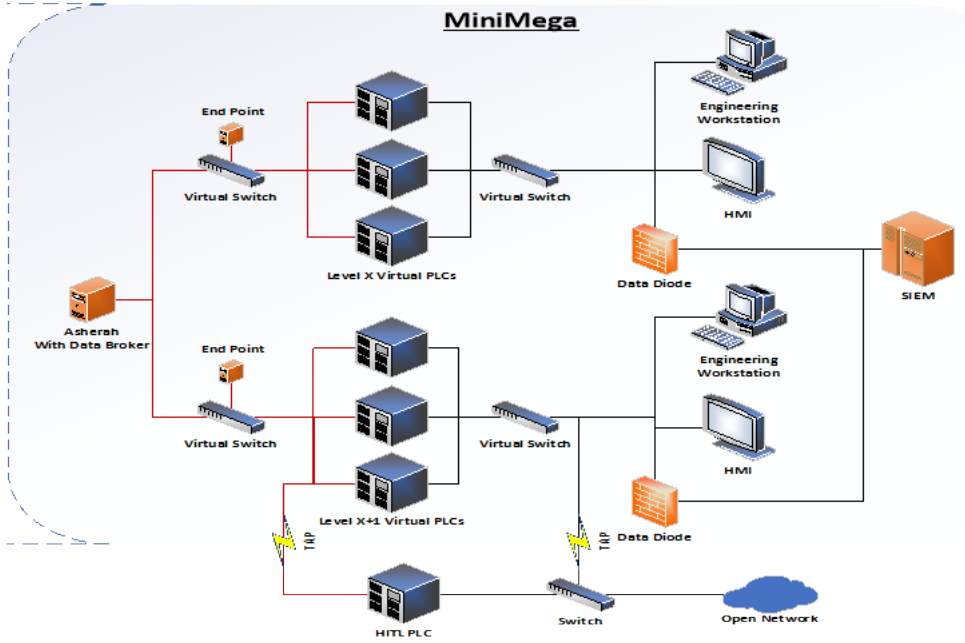


How can we validate the IHT?

Modeling and simulation can be used to validate the IHT



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.

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

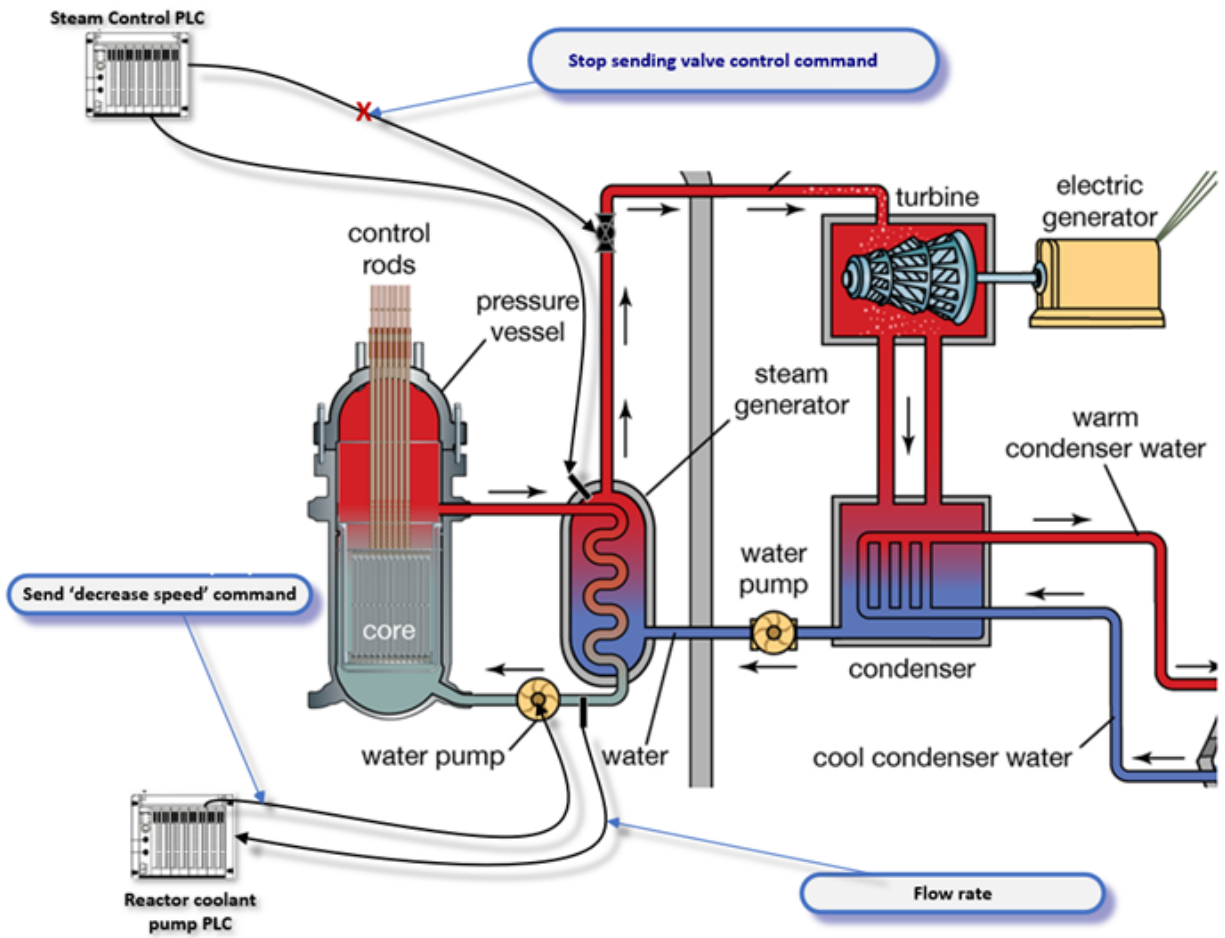


Diagram by: Encyclopedia Britannica (2021)

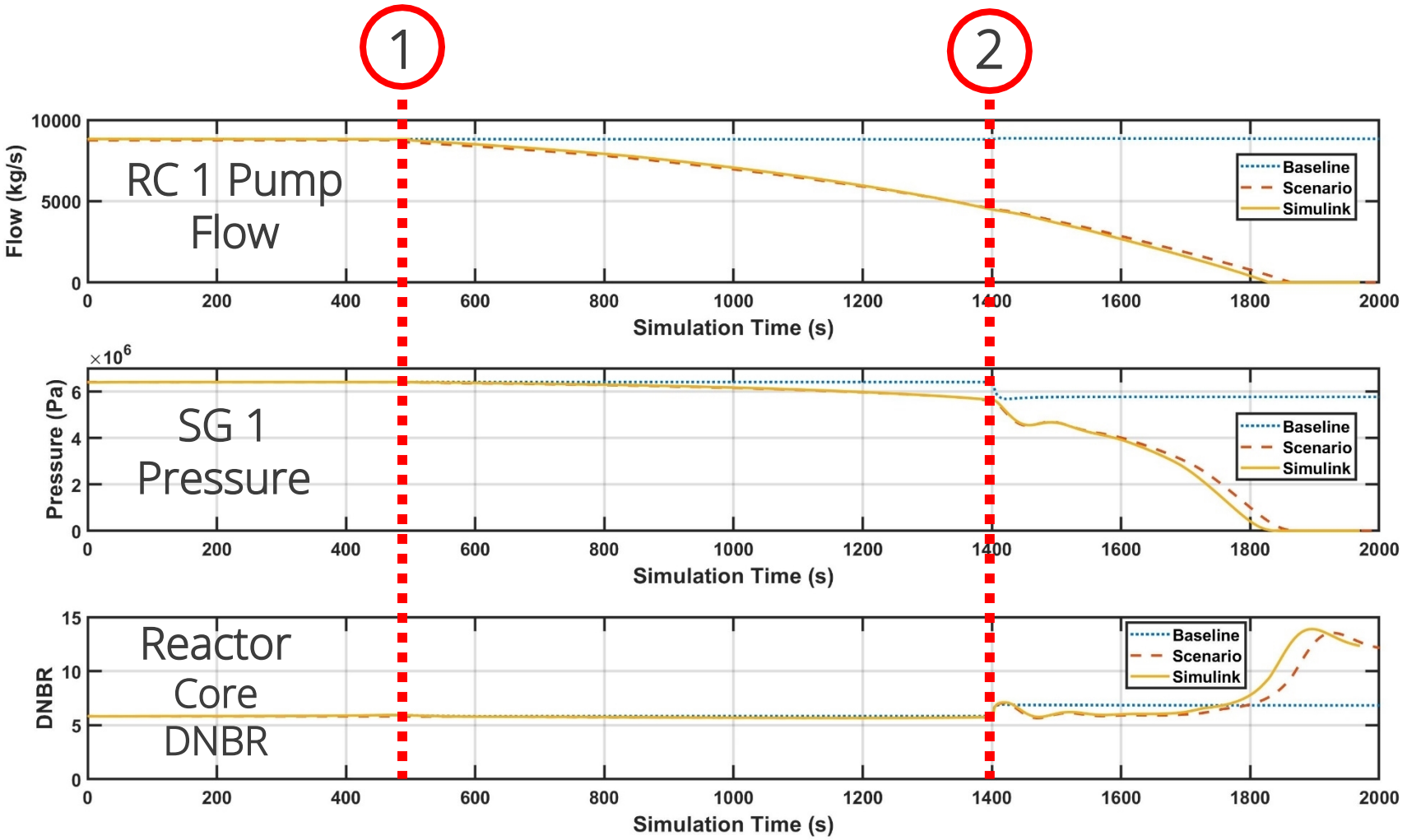
Simulations show the UCA combination causes steam generator pressure to decrease and DNBR to increase

UCA 1:

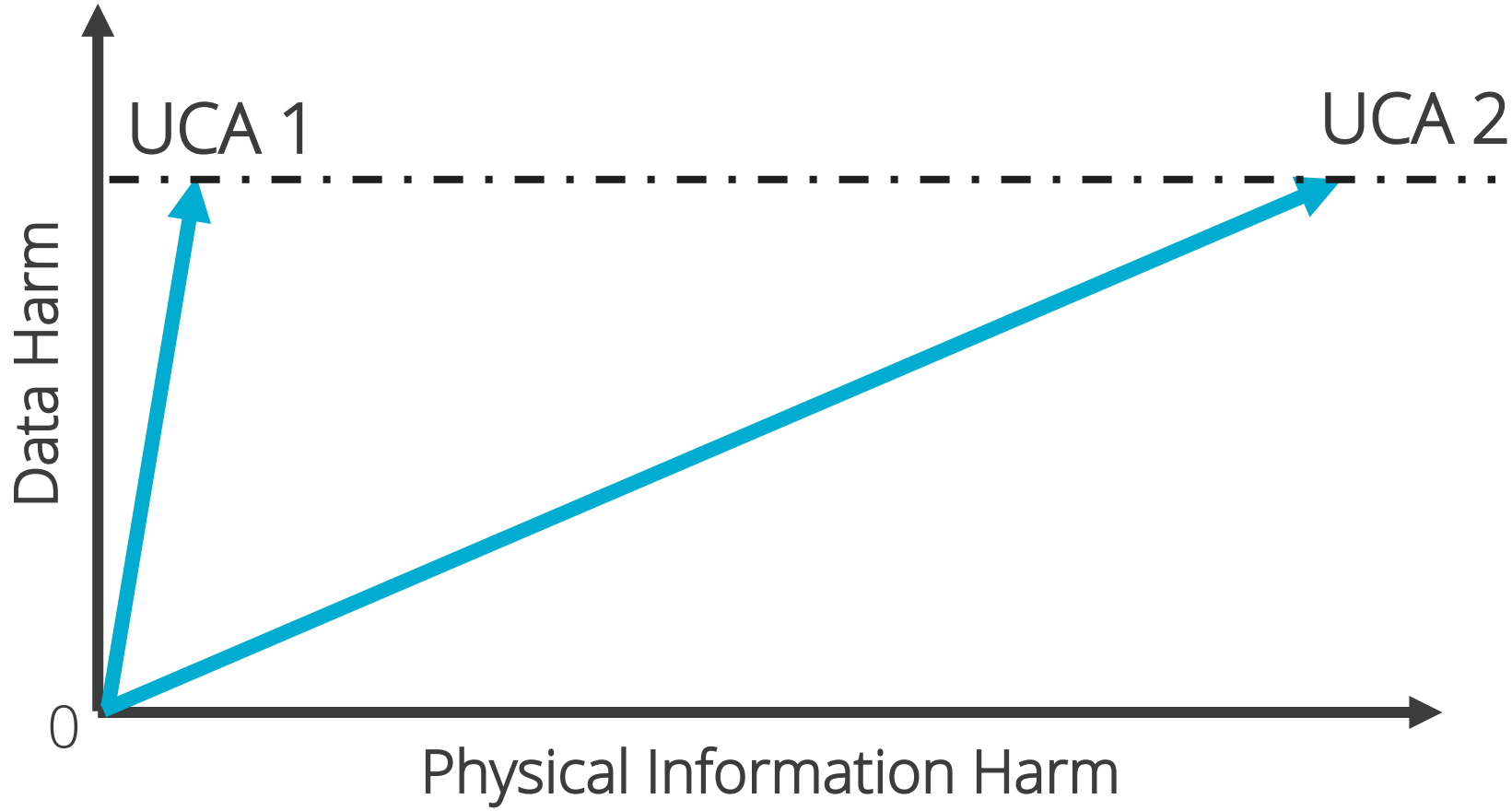
- Initiated at 500 seconds
- Sets input value to PID controller to 11,000 kg/s (desired setpoint ~8800 kg/s)
- Causes PID controller to decrease the pump flow rate

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



UCA 1 and UCA 2 can be represented with IHTs



How can we represent the combination of UCA 1 and UCA 2, and other combinatory effects (e.g. DNBR)?

Future efforts will add further rigor to the IHT

- Investigating units of data harm and physical information harm
- Investigating the use of cumulative harm and rates of harm
- Investigating the effects of timing and sequencing of UCAs
- Apply formal methods and control theory for further rigor

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

4. Future work on the IHT will make it a repeatable cybersecurity analysis tool that produces consistent results regardless of the analyst

Thank you for your time and attention

Contact Information:
Michael T. Rowland
mtrowla@sandia.gov