Demonstration of Advanced Encryption for an Instrumentation and Control System using ARCADE

Daniel Cole
Luis Benitez, Patrick Murphy
Dane Sabo, Robert Lois
University of Pittsburgh

Andrew Hahn, Lee Maccarone
Sandia National Laboratories

September 30th, 2024

University of Pittsburgh | Cyber Energy Center

Hardware-in-the-loop enables real-time testing of hardware by integrating it into a simulated environment. It is most useful for high-value low-volume systems.

Expensive

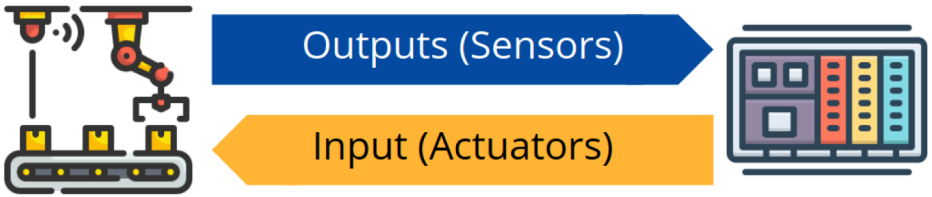
Inaccessible

Dangerous

https://www.nrc.gov/reactors/operating/licensing/renewal/applications/bvalley/bvalley_station.jpg

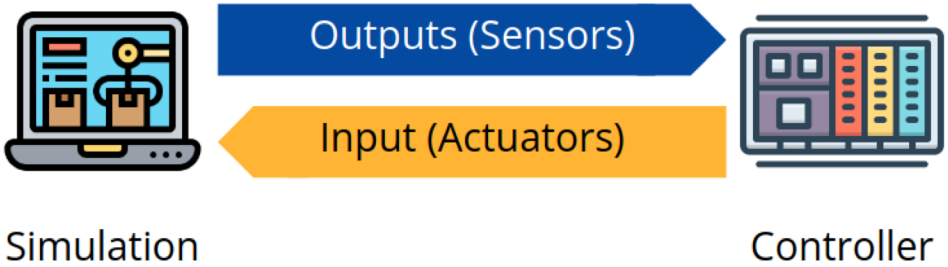
Hardware-in-the-loop simulation integrates real hardware with a virtual simulation environment to test and validate system performance in real-time

This is what a (simple) control system is:

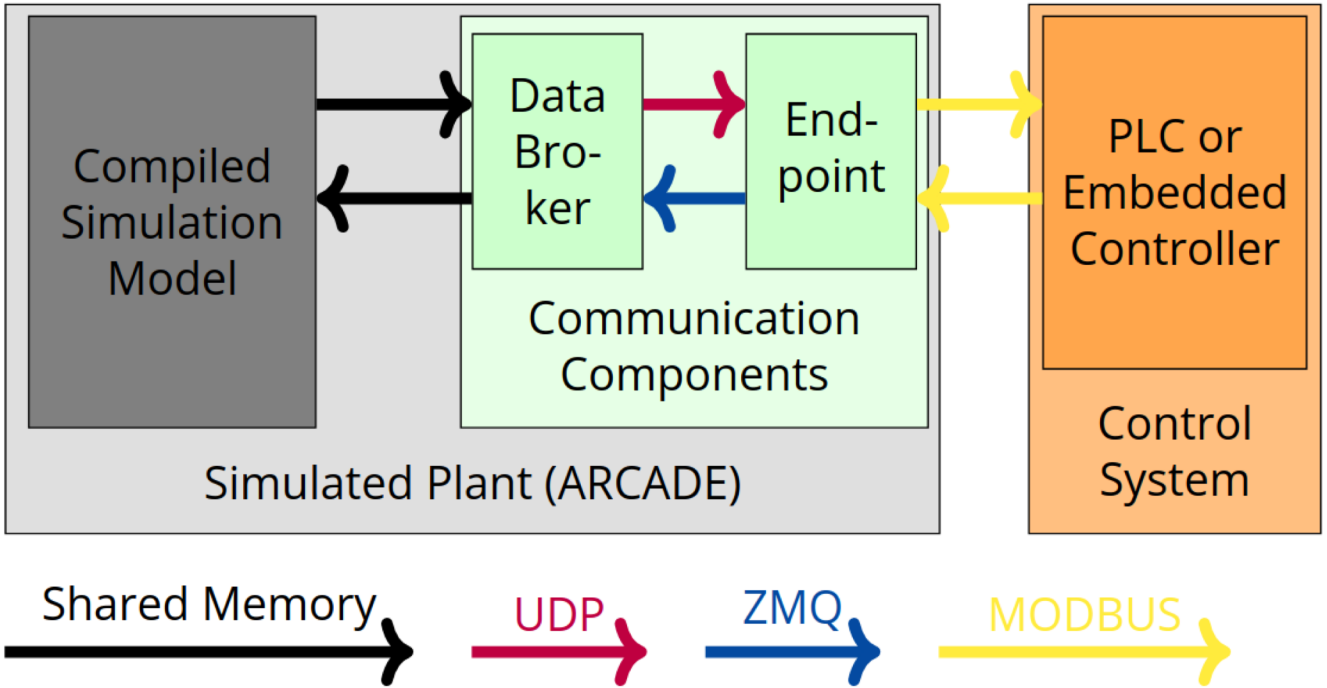


For Hardware-in-the-loop (HiL):

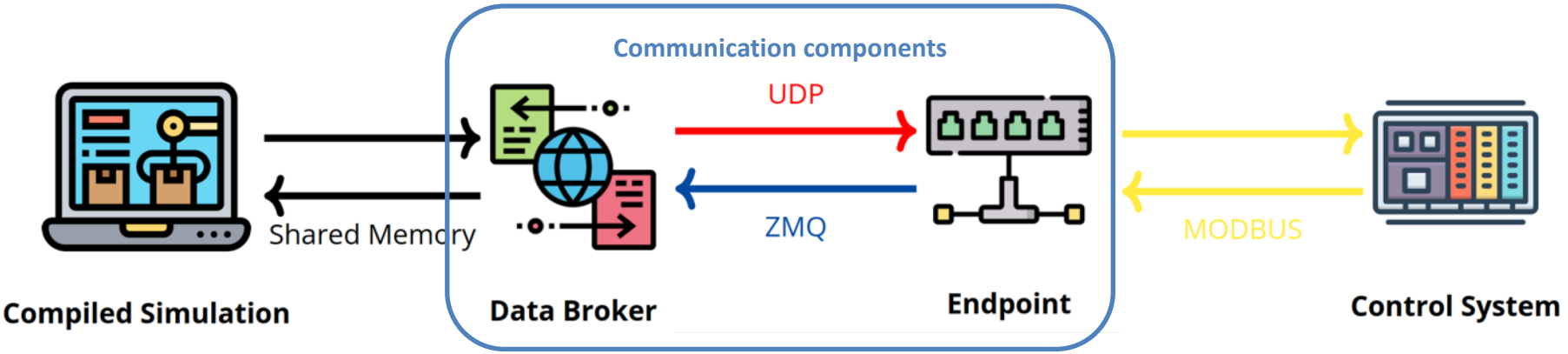
Replace the physical plant with a simulation:



ARCADE is an open-source solution between a pre-compiled simulation model and a control network



The data broker communicates between the simulation and other systems; the endpoint transmits data over Modbus, enabling control and monitoring



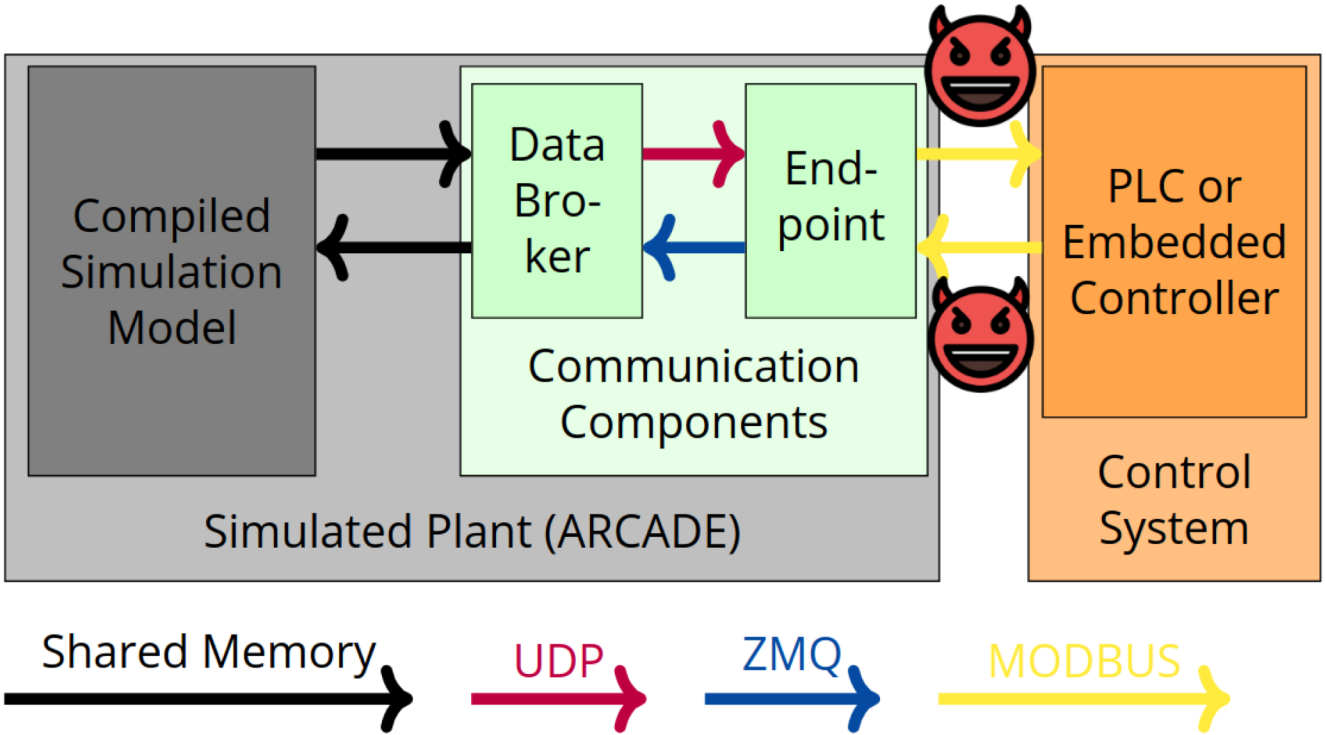
- C/C++ code from SimulinkCoder
- Share memory with the Data Broker

- Reads and writes data to shared memory with the simulation
- Manages the “real-time” pace of the simulation
- Configures the endpoint
- Broadcasts sensor values

- Monitors PLC memory
- Sends PLC control signals to the data broker
- Writes sensor values to the control system
- Listens for updated control signals

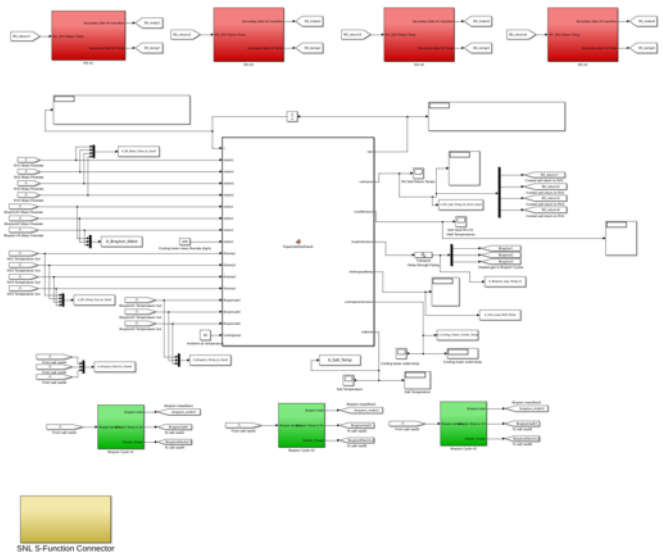
- OpenPLC, real PLC (HiL), or embedded control system
- Has no clue it’s in a simulation

ARCADE allows full control and manipulation of signals, facilitating research into system robustness, cyberattack scenarios, and the measurement of harm

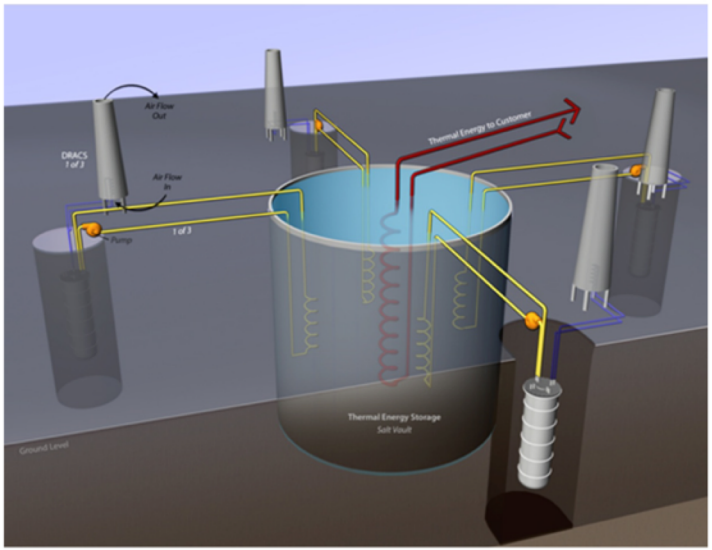


In ARCADE, we have modelled a SmAHTR:
Small Modular Advanced High Temperature Reactor

SmAHTR Simulink model

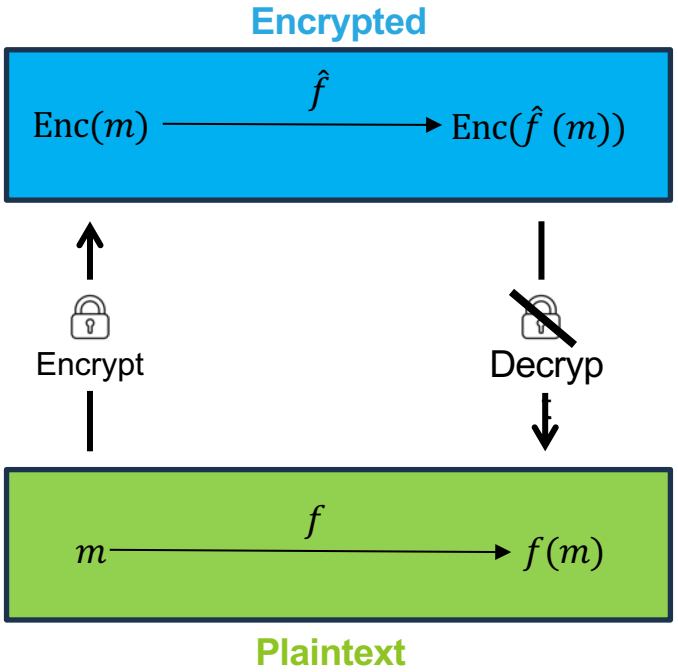


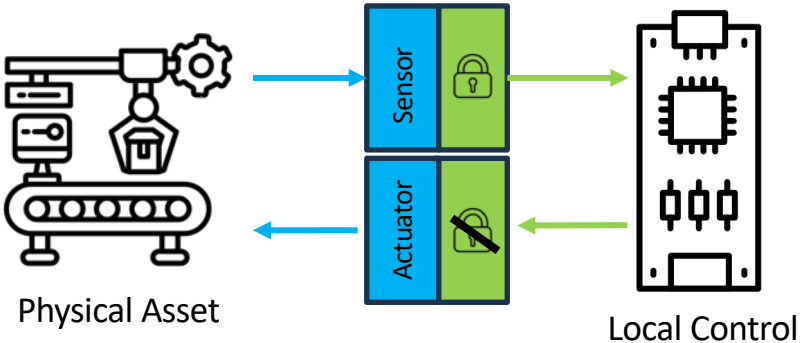
SmAHTR reactors with a salt vault

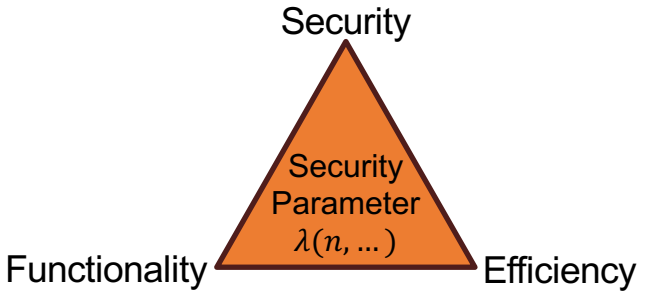


https://info.ornl.gov/sites/publications/files/Pub26178.pdf

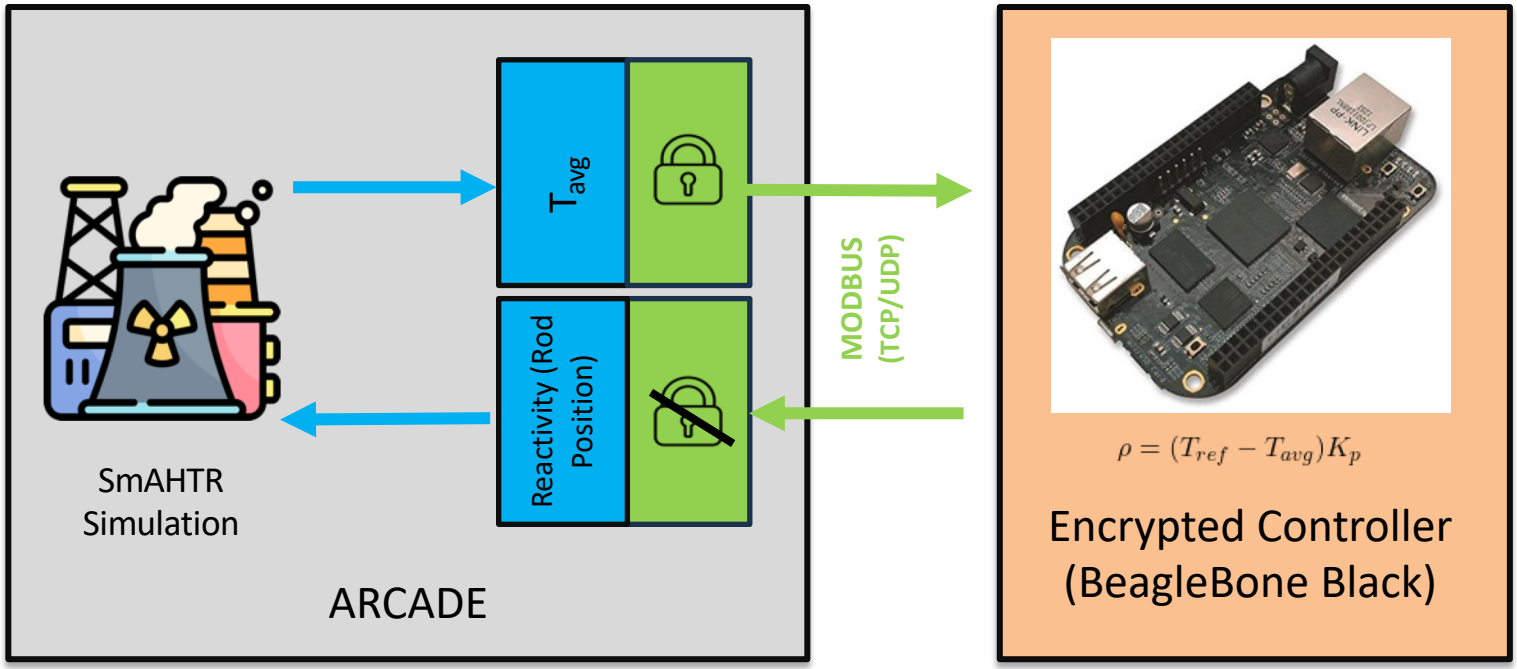
Homomorphic encryption allows computations to be performed on encrypted data without decrypting it



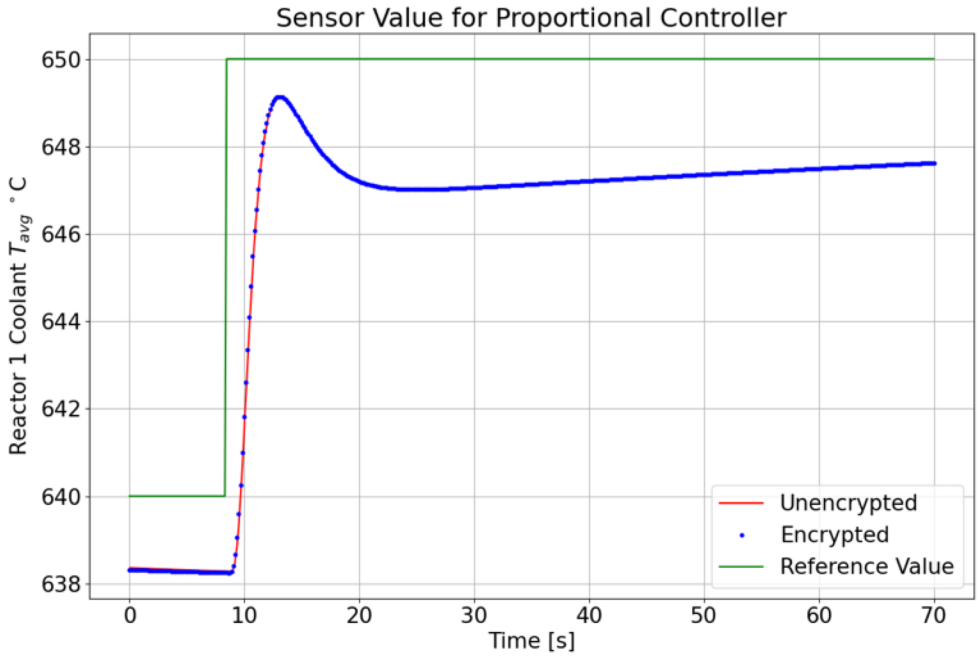




We have used this encryption scheme on a BeagleBone Black connected to the SmAHTR simulation using ARCADE



The encrypted controller is the same as the unencrypted controller

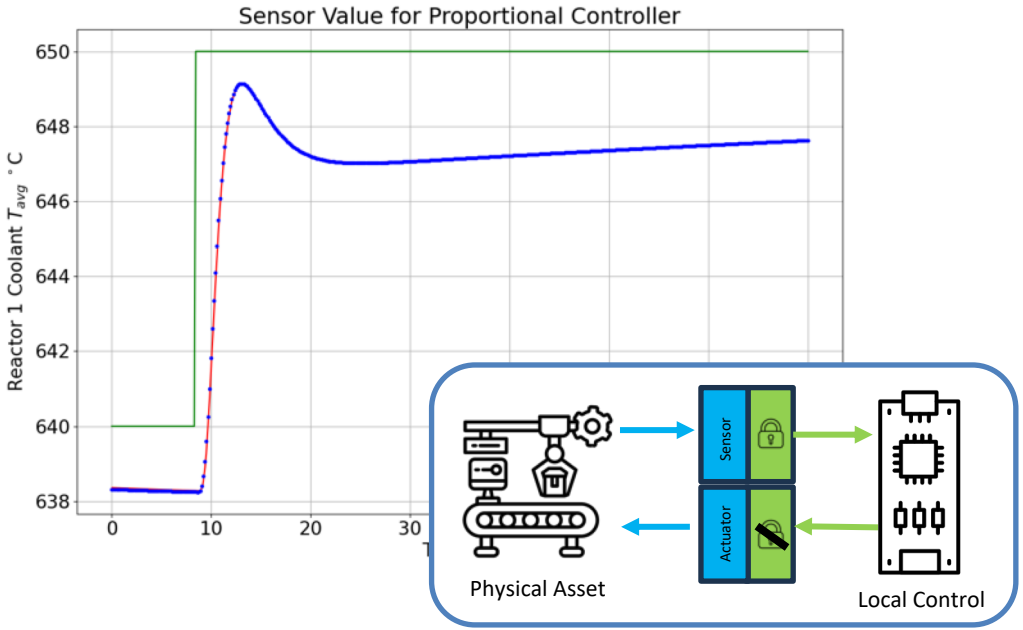


Memory	Unencrypted Controller	Encrypted Controller
Scalar signal (LWE)	4 B	48 B
Scalar gain (GSW)	4 B	3456 B

This demonstrates encrypted control systems for secure control systems in advanced reactor instrumentation and control

Daniel Cole
dgcole@pitt.edu

Questions?



University of Pittsburgh® Cyber Energy Center