CENTER FOR CYBERSECURITY
AT THE UNIVERSITY OF WEST FLORIDA

CAE IN CYBERSECURITY COMMUNITY

On Teaching and Learning Industrial Control Systems Security Using Open Platform Infrastructure

2025 CAE Symposium
Charleston, SC
April 8-10, 2025

Dr. Guillermo Francia, III
UWF Center for Cybersecurity

In the beginning….

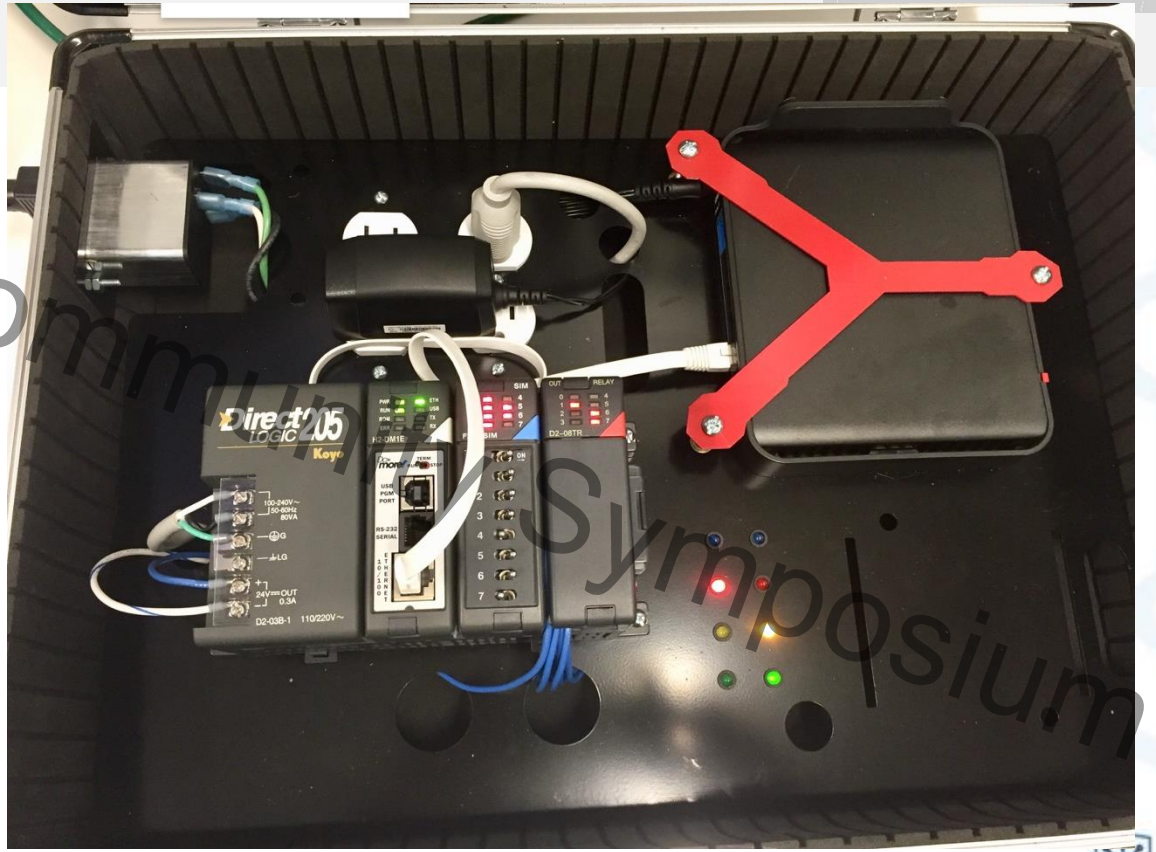
2009: NSF Major Research Infrastructure

Portable RTUs

2011: Security of field devices

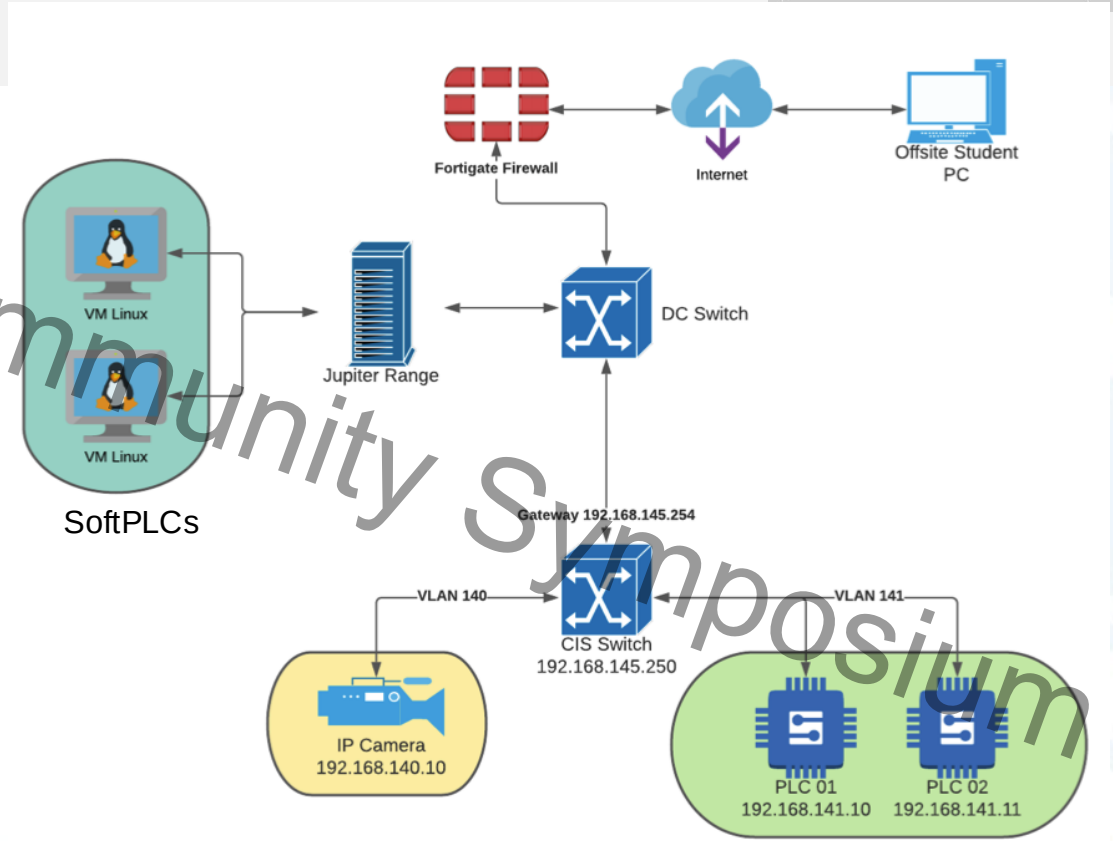
Training Tool Suite

2014: Faculty Development Workshop on ICS-SCADA Security



ICS-Renewable Energy Security Training

2022-2023: UCCS-UWF Faculty Development Workshop Online Training



Contributions to the CAE Community

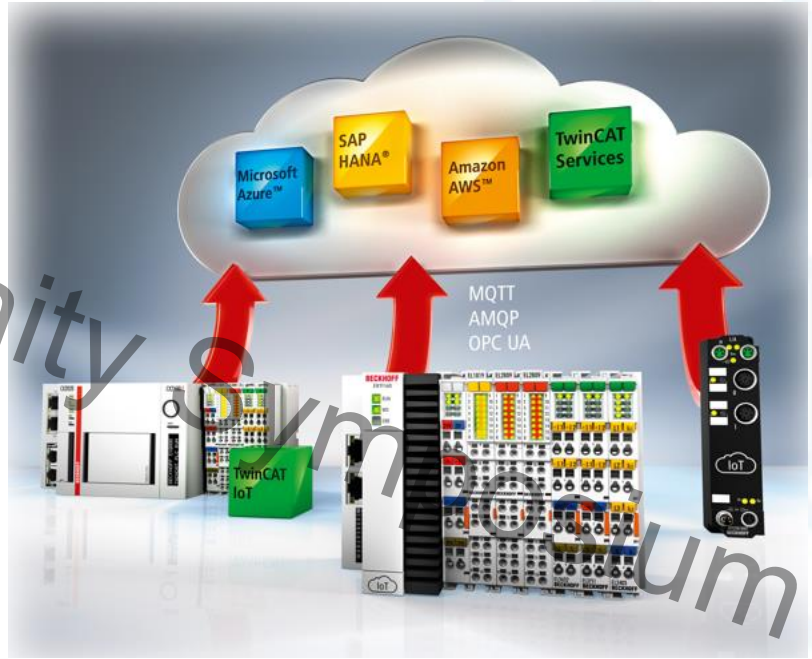
- An affordable infrastructure for an effective ICS security training;
- Useful insights into the design and implementation of ICS Open Platform Infrastructure (OPI);
- A method to validate of ICS vulnerability assessment and security testing tools; and
- A methodology to enable the introduction of up-to-date, real-world ICS security scenarios to augment active learning.

Open Platform Infrastructure (OPI)

- Open Platform Infrastructure enables lightweight containers to securely run in isolation on a given host
- Containers can easily be shared and run on multiple hosts with the assurance that every host gets an identical container that works the same way (Docker (2024))

ICS-Open Platform Infrastructure (ICS-OPI) Design Guidelines

- Works on virtualized PLCs operating on standard ICS protocols;
- Occupies a small footprint and operates in isolation;
- Realizes an IT-OT network infrastructure;
- Facilitates the development of digital twins for ICS security;
- Enables interfacing with an external Human Machine Interface (HMI);
- Facilitates the simulation of ICS attacks and defenses by security purple teams.



ICS-Open Platform Infrastructure (ICS-OPI) Design Implementations

Virtualized PLCs operating on standard ICS protocols

-OpenPLC operating on ModbusTCP, DNP3, and Ethernet/IP

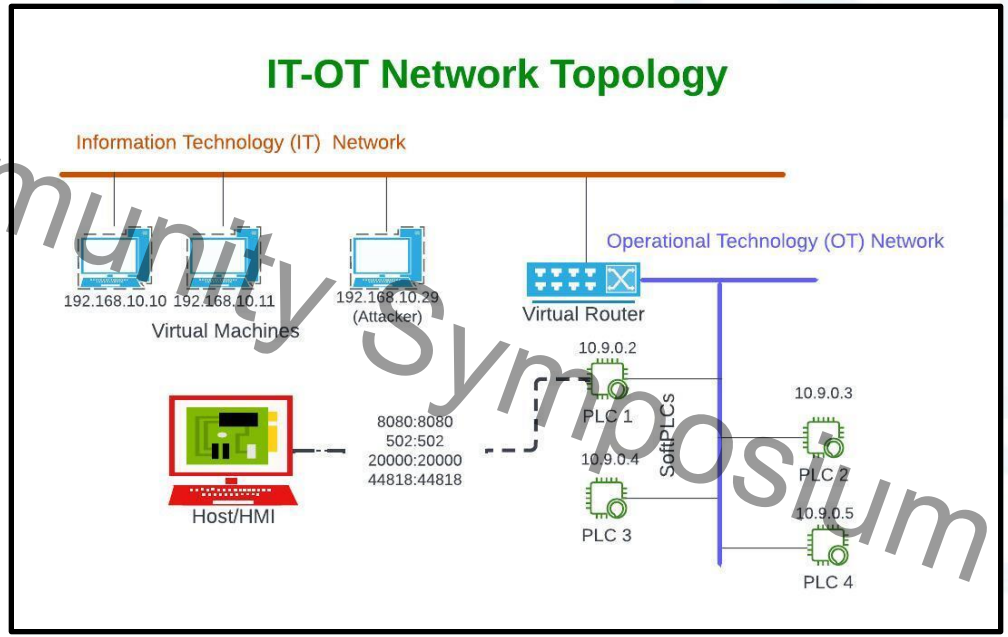
Small footprint in isolation

-Implemented by Docker containers

Realizes an IT-OT network infrastructure

-Implemented by Docker containers with defined network

-Utilizes Docker compose



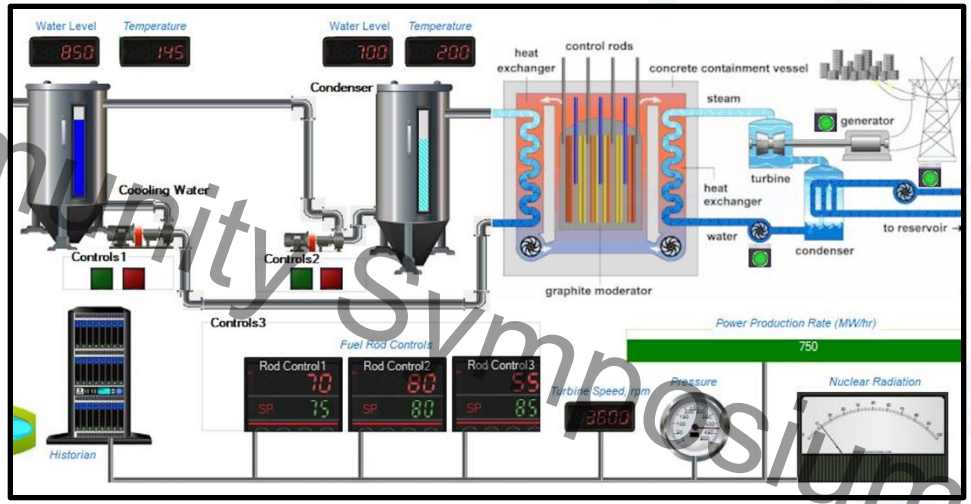
ICS-Open Platform Infrastructure (ICS-OPI) Design Implementations (cont)

Facilitates the development of digital twins for ICS security

-*Combined OpenPLC, Docker containers, Network definitions on Docker-compose, and HMI implementation utilizing AdvancedHMI*

Enables interfacing with an external Human Machine Interface (HMI)

-*The implemented HMI is integrated with the softPLC*

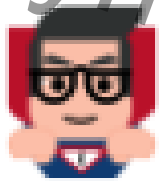


ICS-Open Platform Infrastructure (ICS-OPI) Design Implementations (cont)

Facilitates the simulation of ICS attacks and defenses by security purple teams with the following use cases:

- Reconnaissance
- Lateral movement
- Deep packet inspection
- ICS packet crafting
- Digital forensics
- Intrusion detection and prevention
- Threat intelligence and hunting

The Evolution of ICS Security Training



CLARK

Future Directions

- Expand the collection of ICS security case studies and scenarios to address newly discovered vulnerabilities
- Create virtual OPIs that incorporate devices found in renewable energy and power grid systems
- Expand and improve the creation of digital twins as instruments to carry out enhanced ICS security
- Automate the process of creating security scenarios for the effective utilization of digital twins in security training and education

Forthcoming …

- Faculty development workshop at the UWF Center for Cybersecurity in Pensacola, FL. Travel stipend up to $1200 afforded to faculty participants in July 2025.
- Complete OPI-ICS Security curriculum will be shared with the CAE community utilizing the CLARK System.

Acknowledgements

This work is partially supported by a subaward from the University of Memphis through a National Security Agency award under Federal Grant Number H98230-21-1-0319. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein.

2025 CAE Community Symposium