SAND2023-05083C

National Nuclear Security Administration

United States
Department of Energy
National Nuclear Security Administration

International Nuclear Security

Open-Source Emulation Platform for Hands-on Cyber Attack Training and Experimentation

June 19th 2023

Andrew S. Hahn (SNL)
Romuald Valme (SNL)
Michael Rowland (SNL)
Shannon Eggers (INL)

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

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.

Importance of Opensource

- Allows greater collaboration on multidisciplinary problems
- Grows the cybersecurity community
- Provides equal access to educational materials
- Produces projects with greater global impact
- Increases the longevity of tools and resources
- Reduces over all effort to produce and maintain tool sets

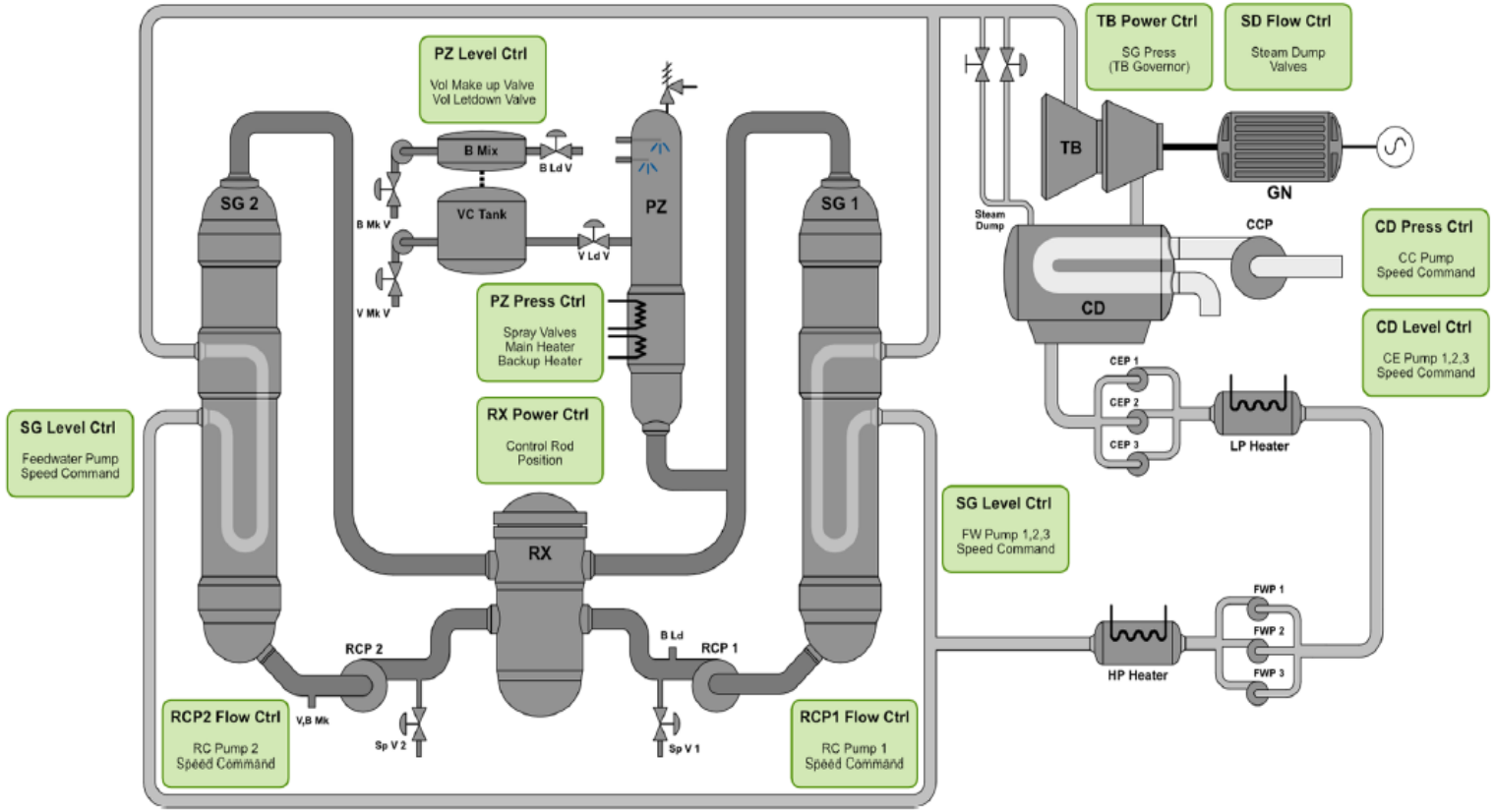


Image: Silva RB, Shirvan K, Piqueira JR, Marques RP. Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment. International Conference on Nuclear Security (ICONS), 10-14 Feb 2020 in Vienna Austria 2020.

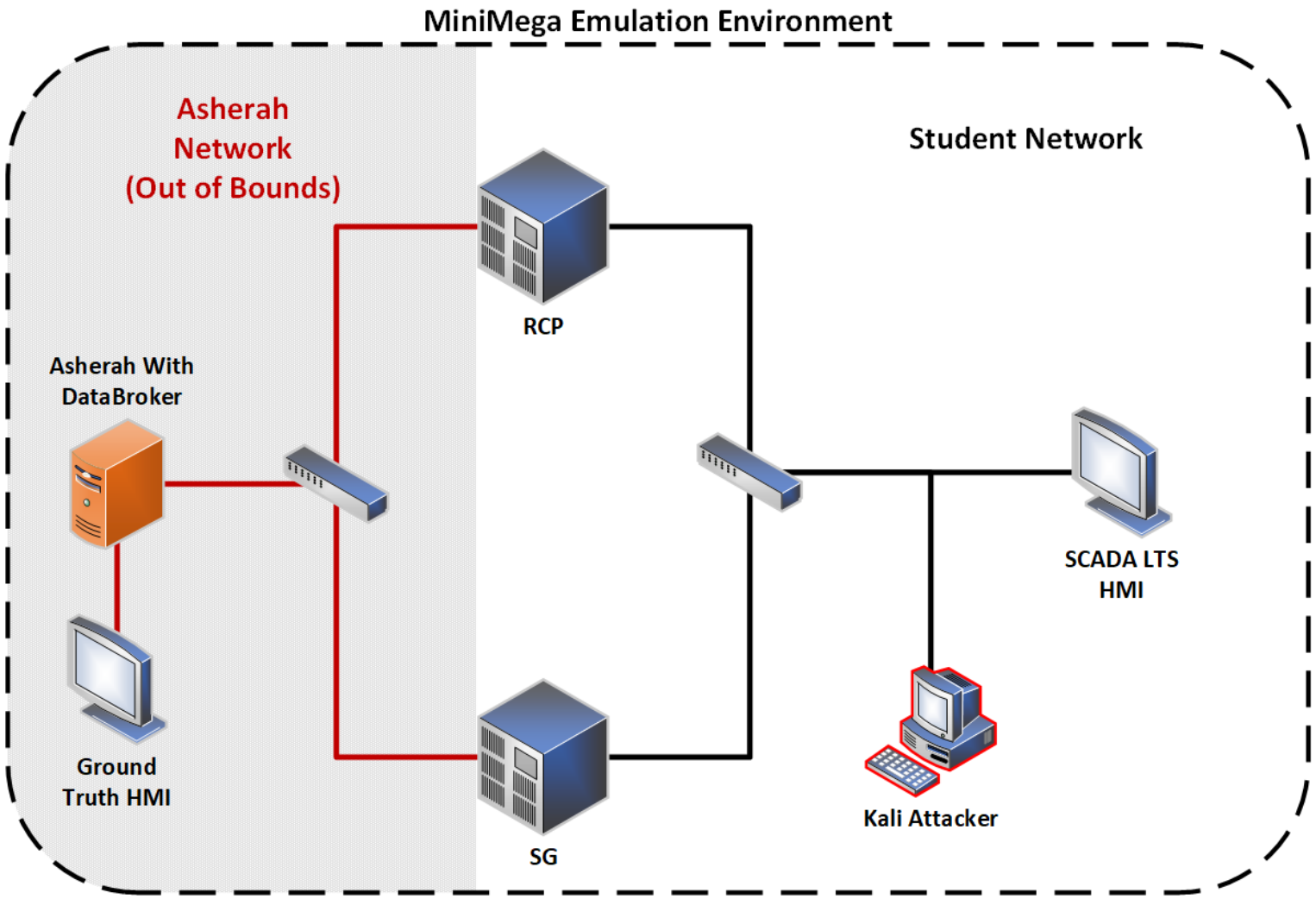
Key Platform Elements

Components	Technology
Virtualization Environment	minimega
Physics Integrator	Sandia DataBroker
Cyber Attack Simulator	ManiPIO & Kali Linux
PLC Runtime Environment	OpenPLC
SCADA Interface	scada-LTS
Physics Simulation	Asherah* Nuclear Power Plant Simulator

* Not Included

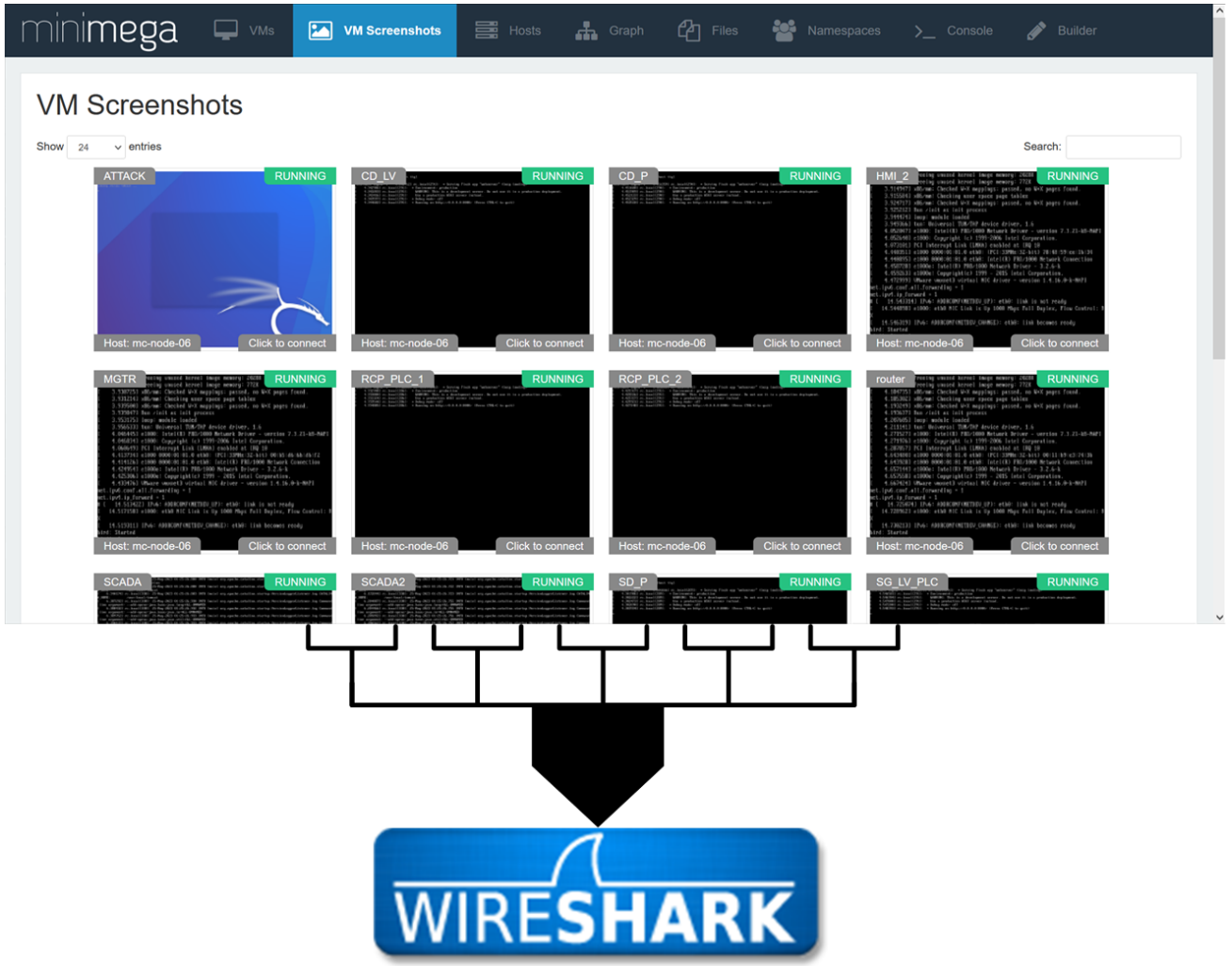
DOE-INS Brazil Course Environment

- Opensource
- Portable
- Stable
- Minimal hardware requirements
- Interactive control system and NPP physics
- Software defined network topology



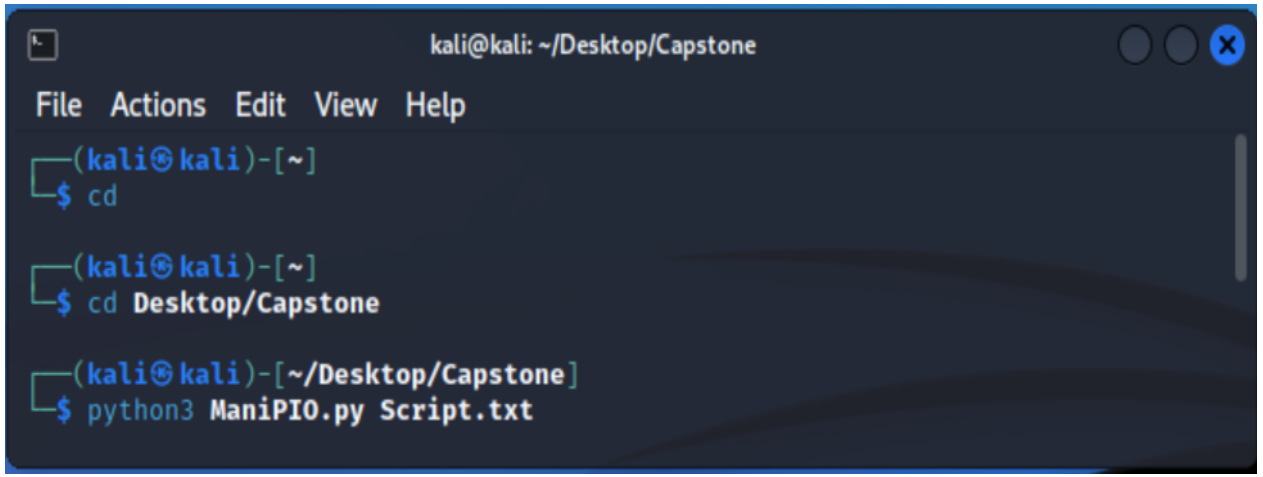
Minimega Transparency

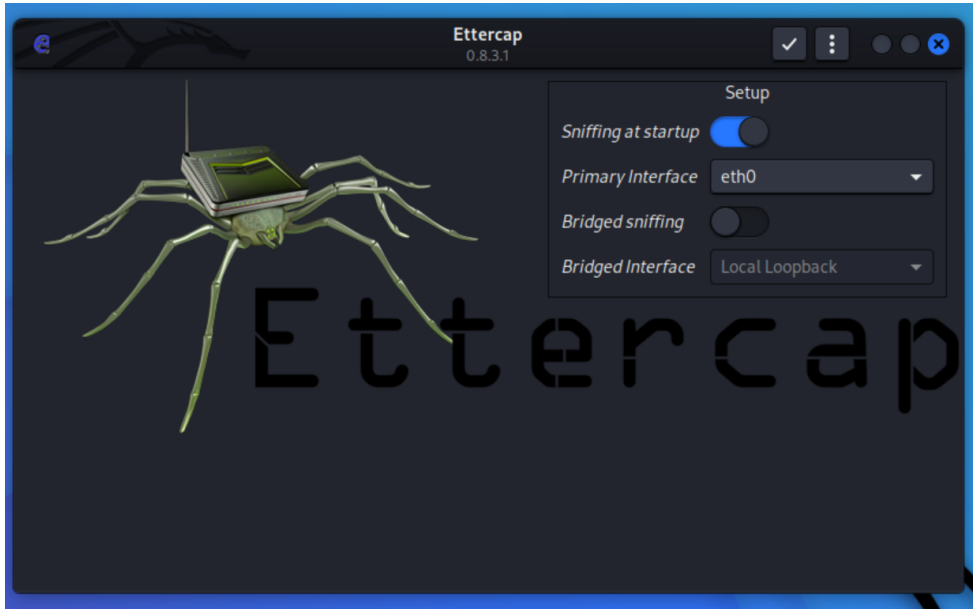
- All interfaces within Minimega are capturable
- Wireshark is used to view network traffic across the entire topology
- File structures and processes are inspectable live

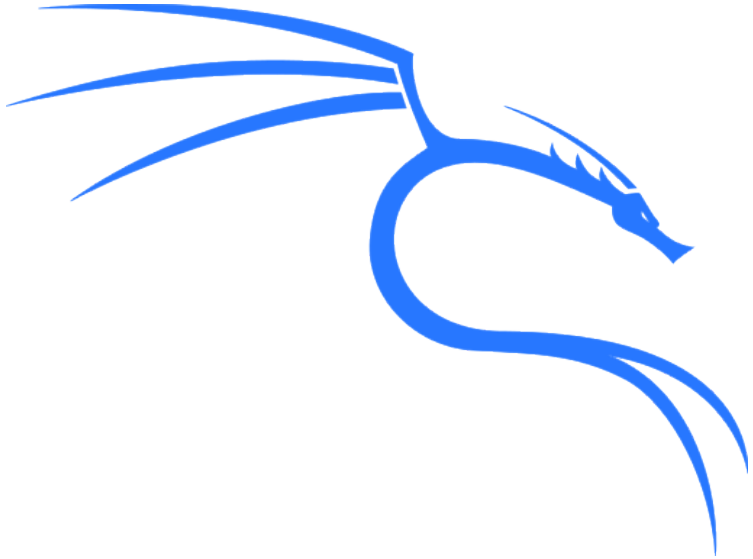


Course Objectives

- Students are asked to be a hacker in the class and perform a series of attacks
  - Alter memory values on Programmable Logic Controllers (PLCs)
  - Man-in-the-Middle attack against the SCADA Human Machine Interface (HMI)

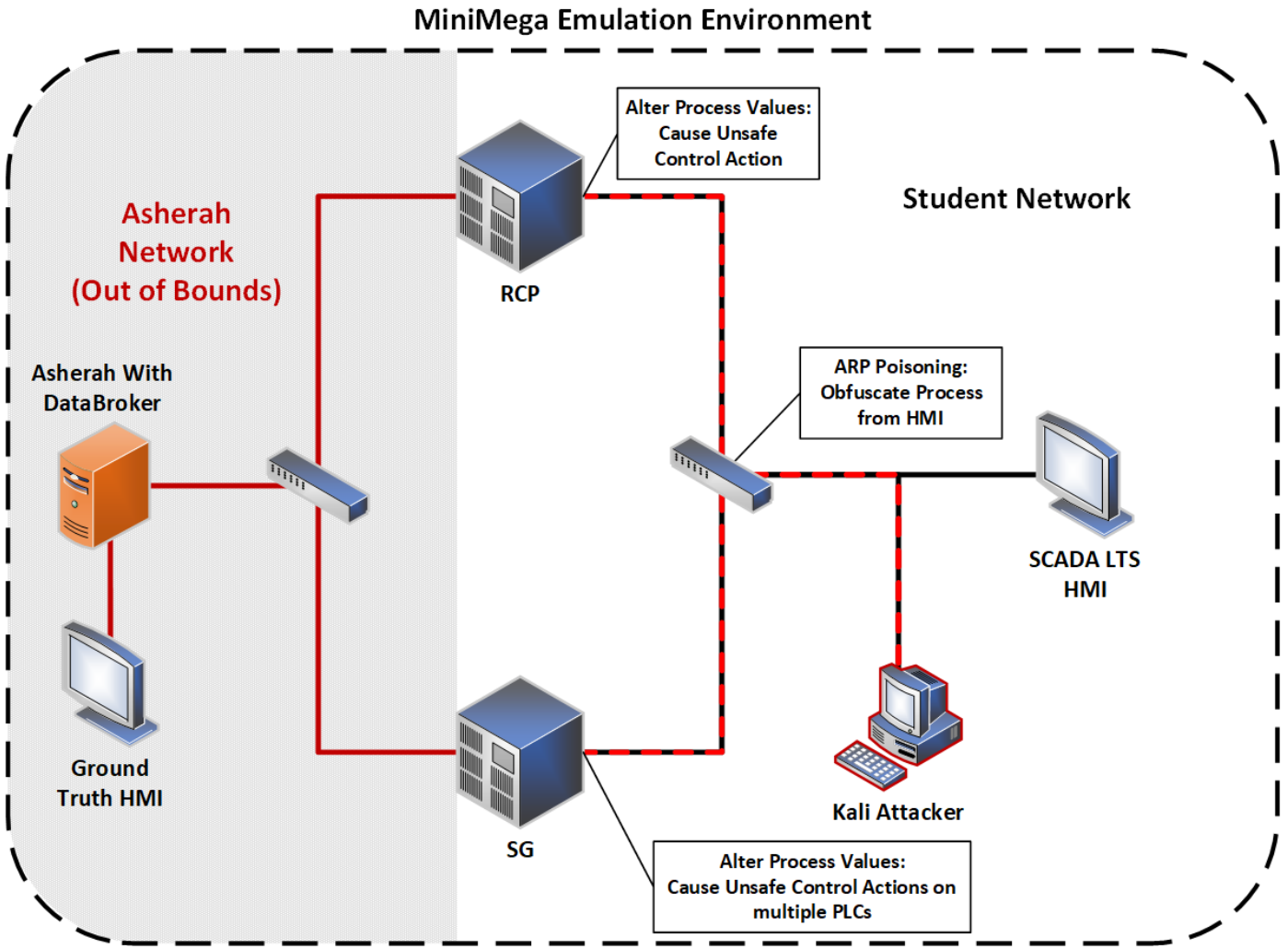






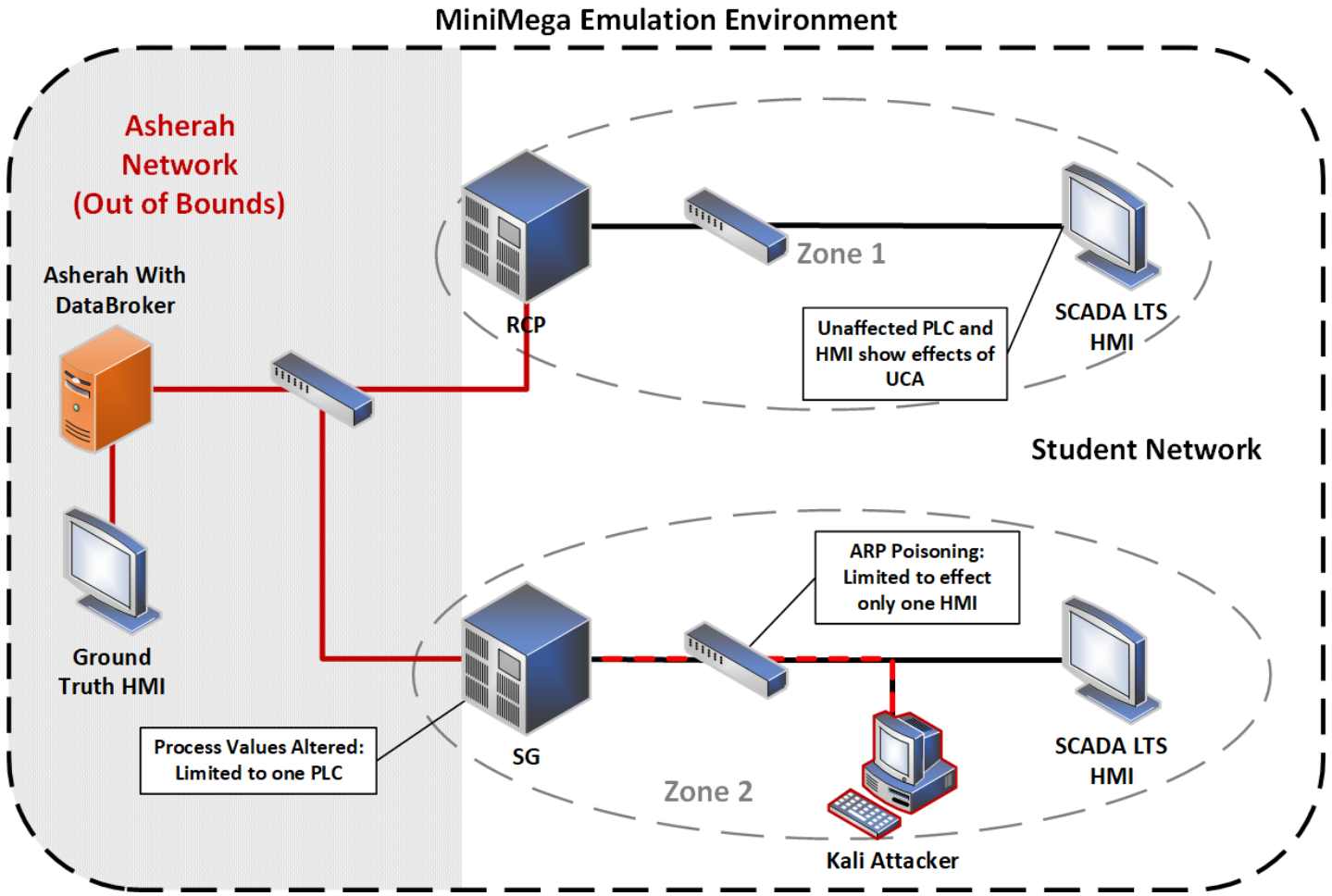
Attack Analysis

- What did this attack do?
  - Obfuscate information from the PLCs to the HMI
  - Altered sensor information on the PLCs to disrupt the plant
- How can this attack be prevented?
  - How can we make this attack impossible?
  - How do we give operators good information while making dangerous attacks as difficult as possible?



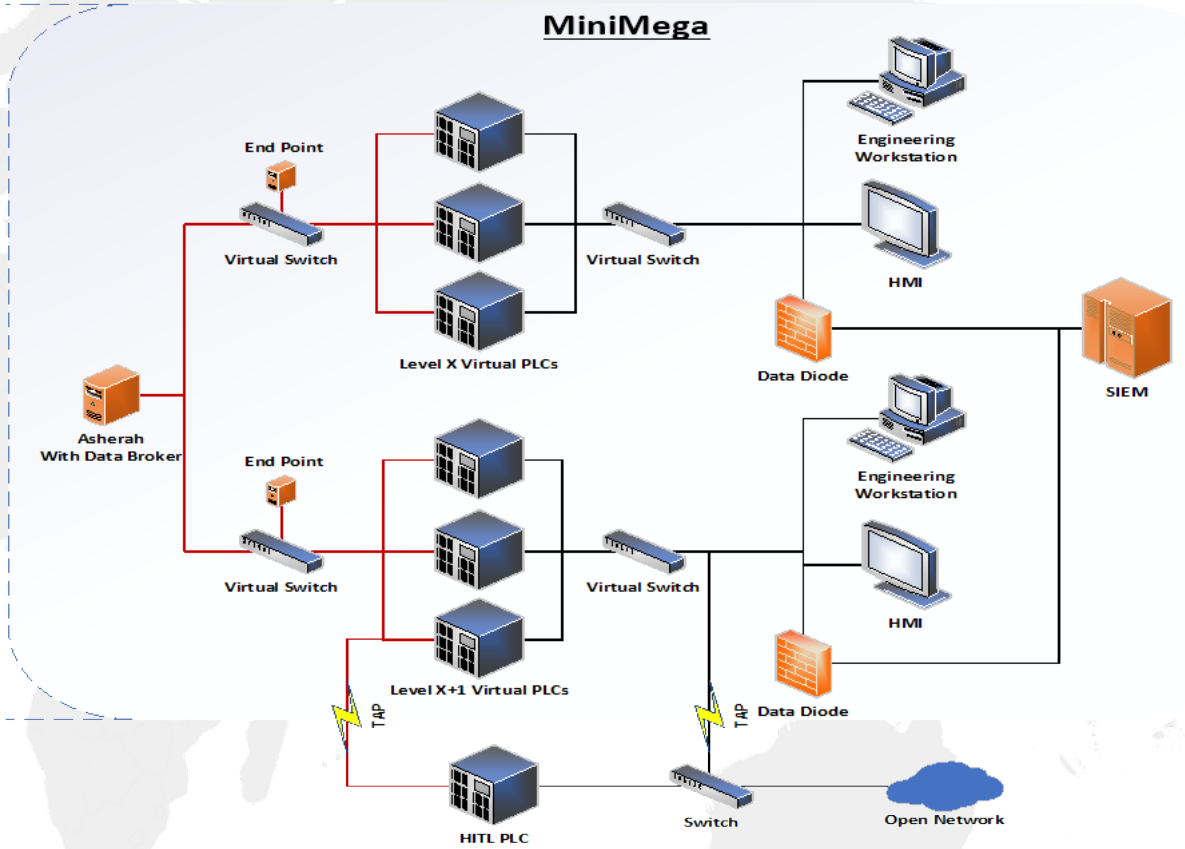
Protect Against Attacks

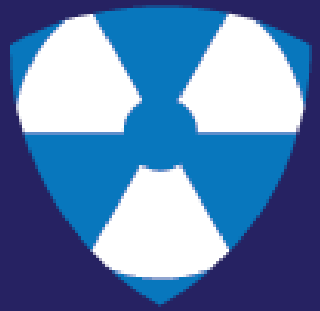
- Students must apply the knowledge from the course to create a better network
- Minimega allows the modification of the network on the fly
- Students run the attacks again on their modified network to see the difference



Current & Future Work

- Reducing size
  - Self-assembling system
  - Ease distribution
- Resource optimization
  - Containers
  - Larger more complex networks
- Automation
  - Scripts to reduce command line need
  - Pre-canned network topologies reduce complexity
  - Opensource GUI interfaces for Minimega





INS International Nuclear Security

Reducing Risk of Nuclear Terrorism