University of Idaho
College of Engineering

ISAAC: THE IDAHO CPS SMART GRID CYBERSECURITY TESTBED

YACINE CHAKHCHOUKH

Co-Authors:

Ibukun Oyewumi, Philip Richardson, Hari Challa, Brian K. Johnson, and Daniel Conte de Leon

INTRODUCTION

A WORLD OF CRITICAL INFRASTRUCTURE

- Critical infrastructure such as the electric power grid provides real-time data processing from local or remote locations.
- Increase in newer cyberphysical system (CPS) feature mechanisms.
- Digitalized movements and automation advancements.
- Convergence of Information Tech and Operational Tech networks

INTRODUCTION

PROBLEM

- Smart grids are a vital part of critical infrastructure.
- Modern SCADA networks are prone to cyber attacks.
  - Lack of tools to implement verifiable security.
  - Legacy insecure devices are still in use.
  - Enhanced exposure and vulnerability with increased connectivity

CHALLENGE

SECURING CYBER PHYSICAL SYSTEMS

To create a secure and resilient CPS:

- Testing and validation in a real world environment.
- Difficult or Impossible to test in a real environment.
- Fully simulated tests may not provide accurate results.
  - Complex and real time interactions.
  - Device characteristics and vulnerabilities.

PROPOSED SOLUTION

REALISTIC CPS TESTBED

To emulate real-world-like vulnerability scenarios :

- A Testbed that can fully represent a CPS organization.
  - Hardware-in-the-loop, not just hardware-simulation.
- Enable small-scale but real experiments.

IDAHO CPS SCADA CYBERSECURITY TESTBED (ISAAC)

- Adaptive and reconfigurable smart grid testbed.
- Consists of real automation controllers along with:
  - IEDs, PMUs, SCADA software, analytics platforms etc.
- Models emulate smart grid power system cases.
- Enable real vulnerability assessment.
- Enable Mitigation development
- Facilitates cybersecurity research and education.

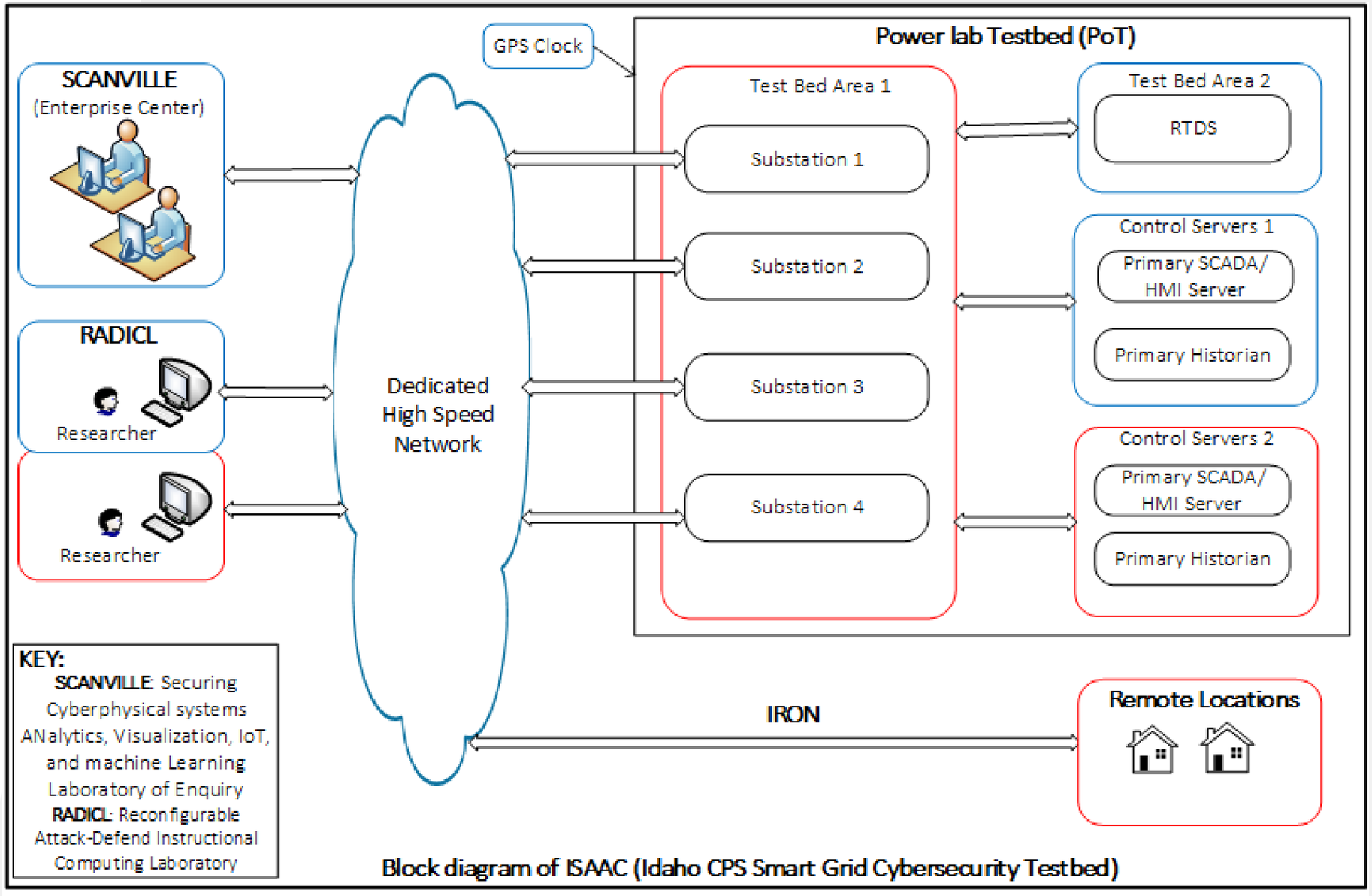
CHALLENGES

- Funding: State of Idaho, MJ Murdock.
- Team: build multidisciplinary team (Faculty, staff).
- Usable security and safety.

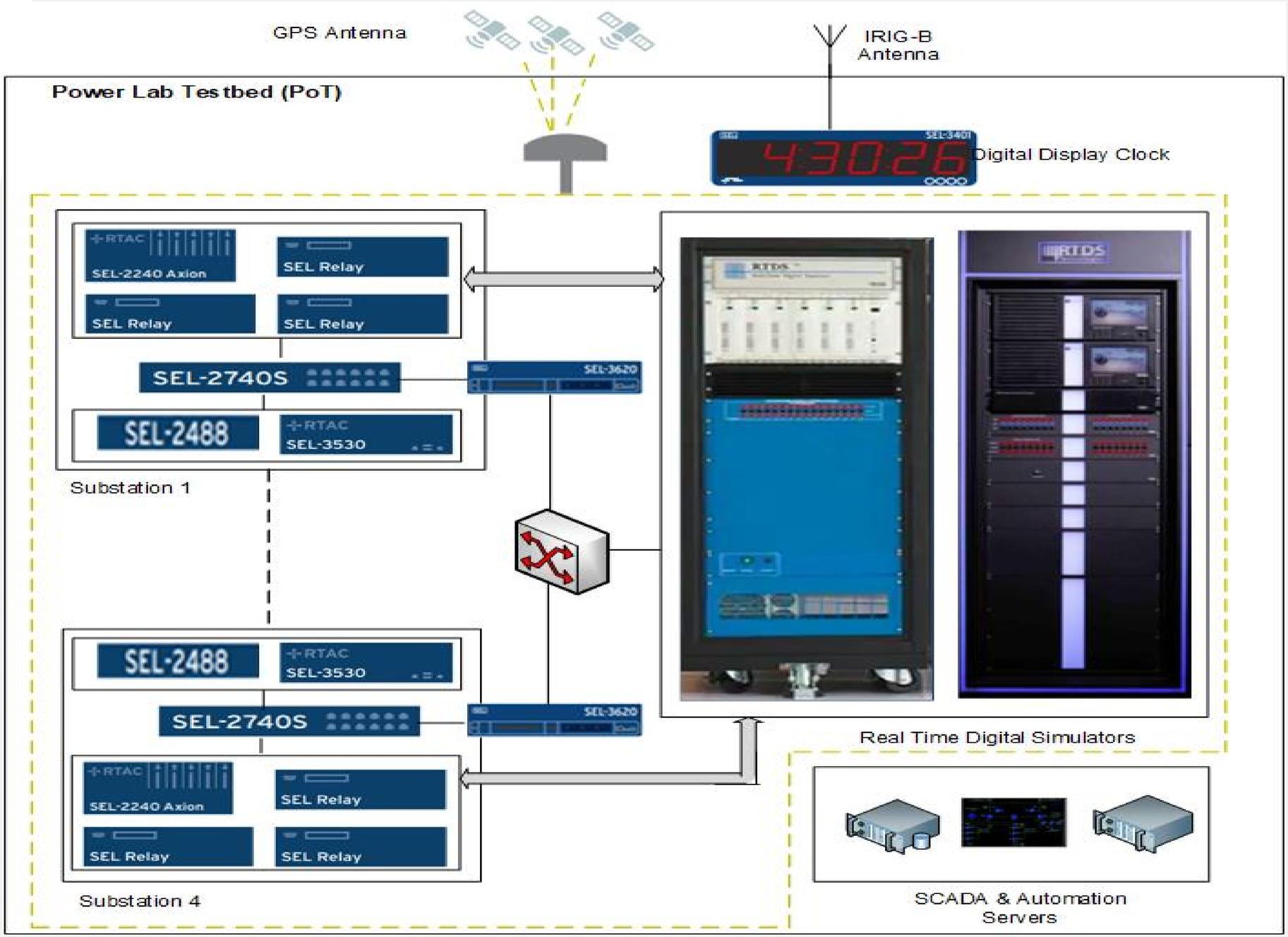
ISAAC SYSTEM COMPONENTS

- Power lab Testbed (PoT):
  - RTDS, 4 small Substations, SDN switch, firewall, PMU, GPS clock, RTAC, relay and other control devices.
- Reconfigurable Attack-Defend Instructional Computing Laboratory (RADICL):
  - Computing environment for forensics and penetration testing.
- Securing Cyberphysical systems ANalytics, Visualization, IoT, and machine Learning Laboratory of Enquiry (SCANVILLE)
  - Analytics and Visualization
  - Hybrid: Control and Cyber views.

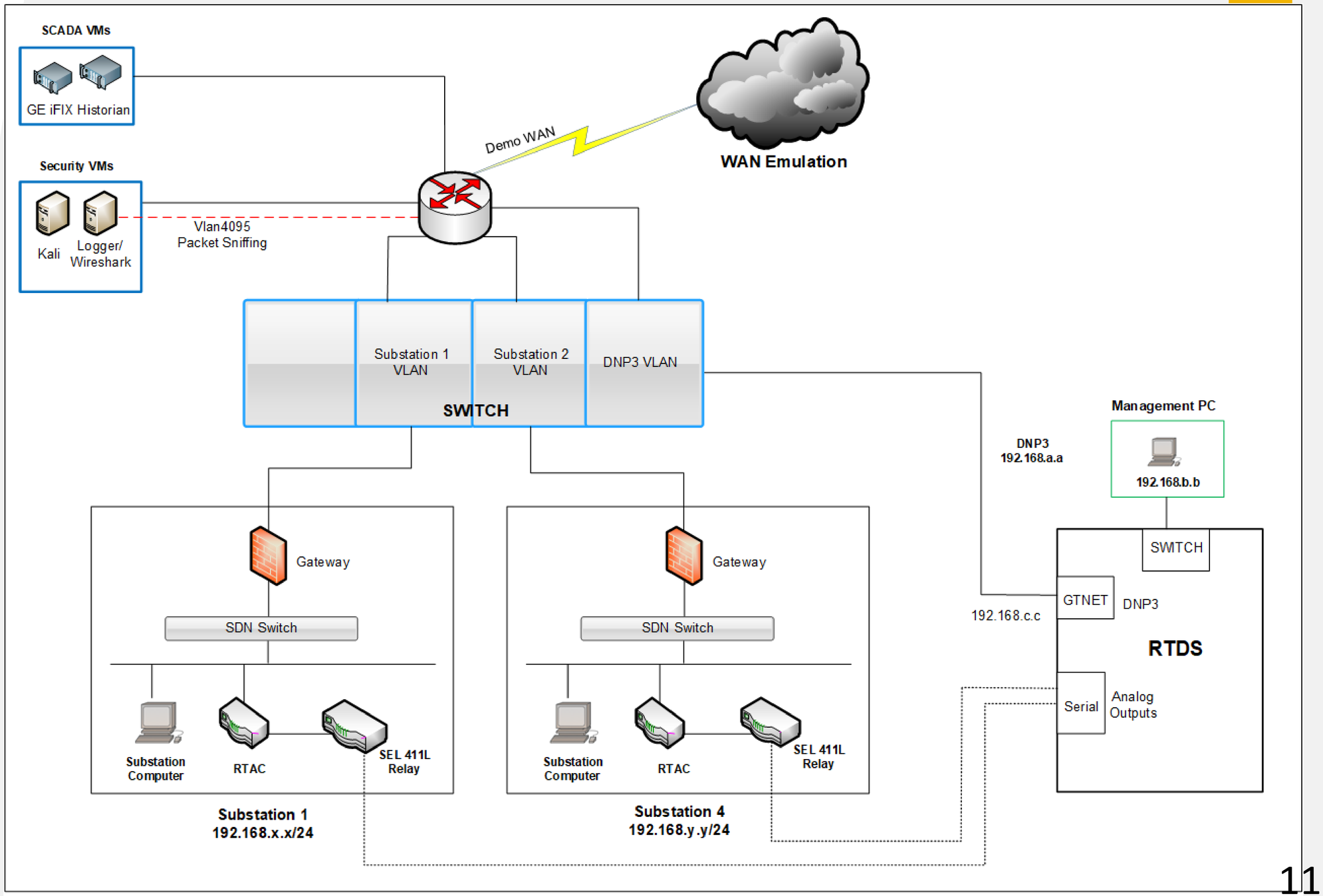
ISAAC: BLOCK DIAGRAM



POWER LAB TESTBED

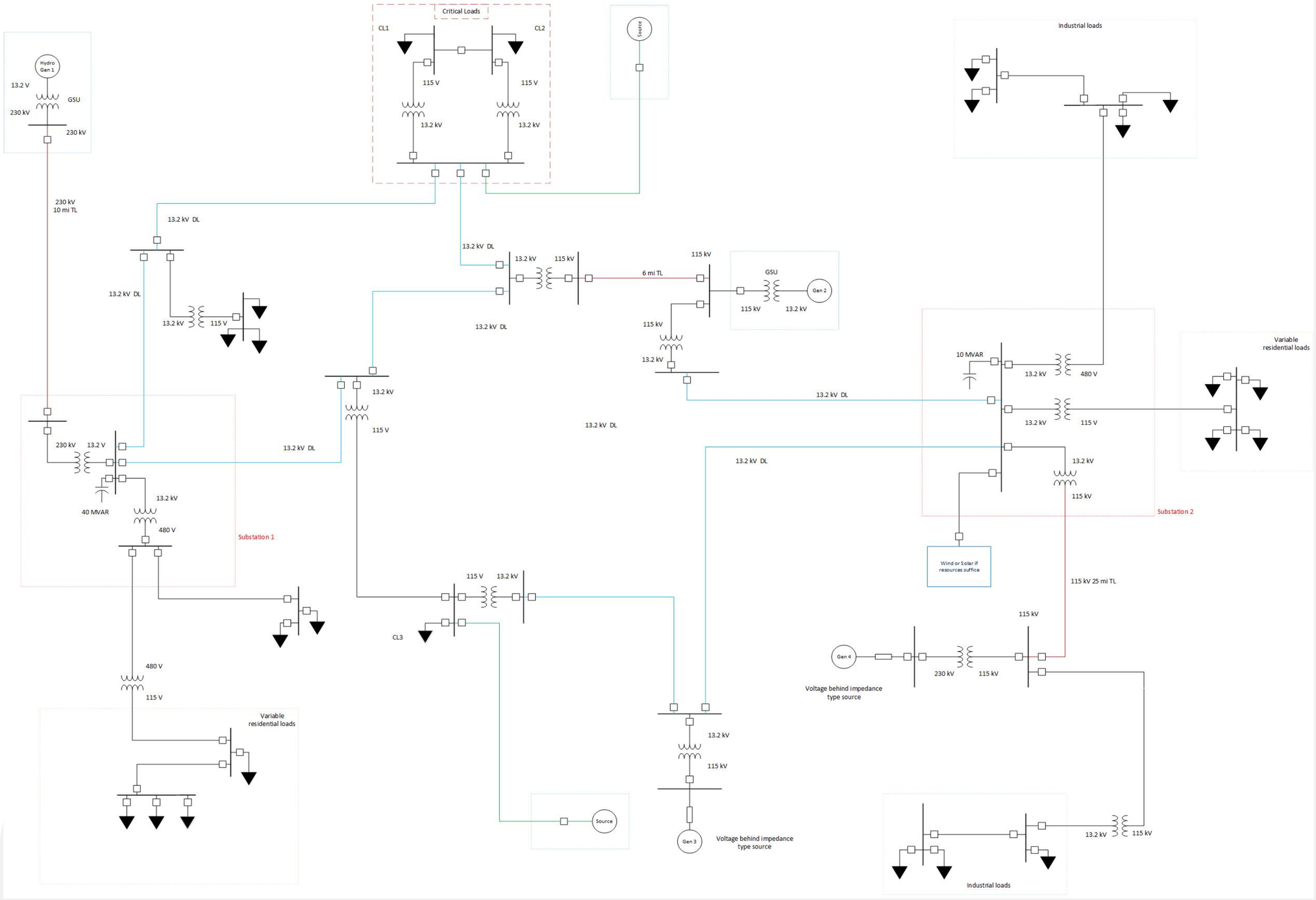


DATA FLOW

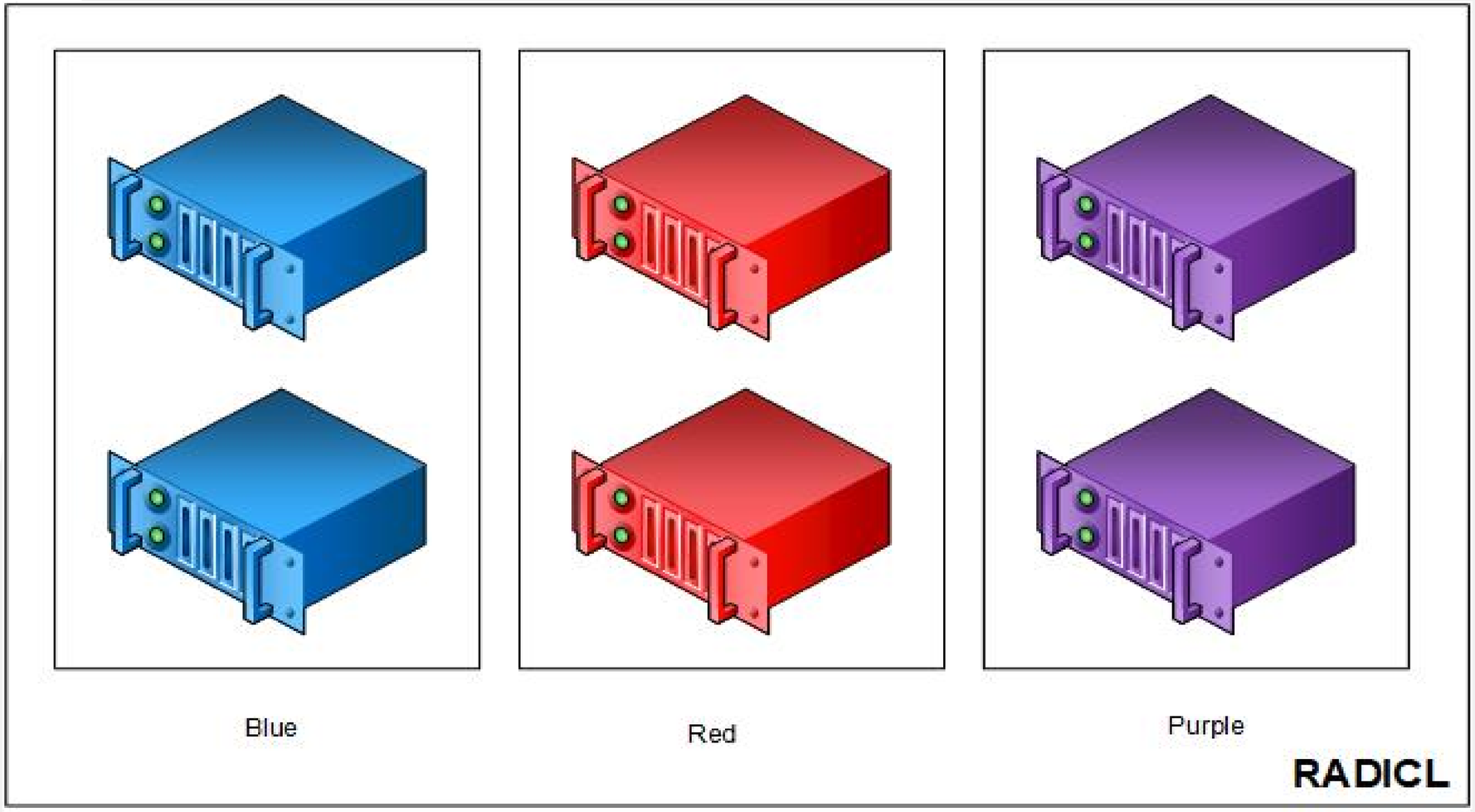


RESILIENCE RESEARCH DATAFLOW DIAGRAM

EXAMPLE SINGLE LINE DIAGRAM



RADICL



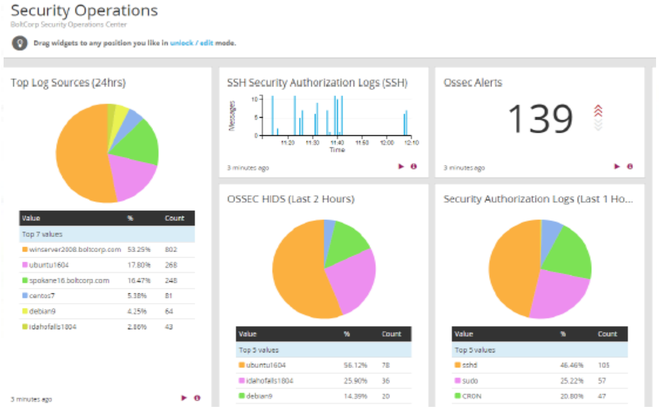
- Blue: Teaching, non-attack zone
- Red: Penetration testing tools
- Purple: Infrastructure zone

SCANVILLE

Visualization

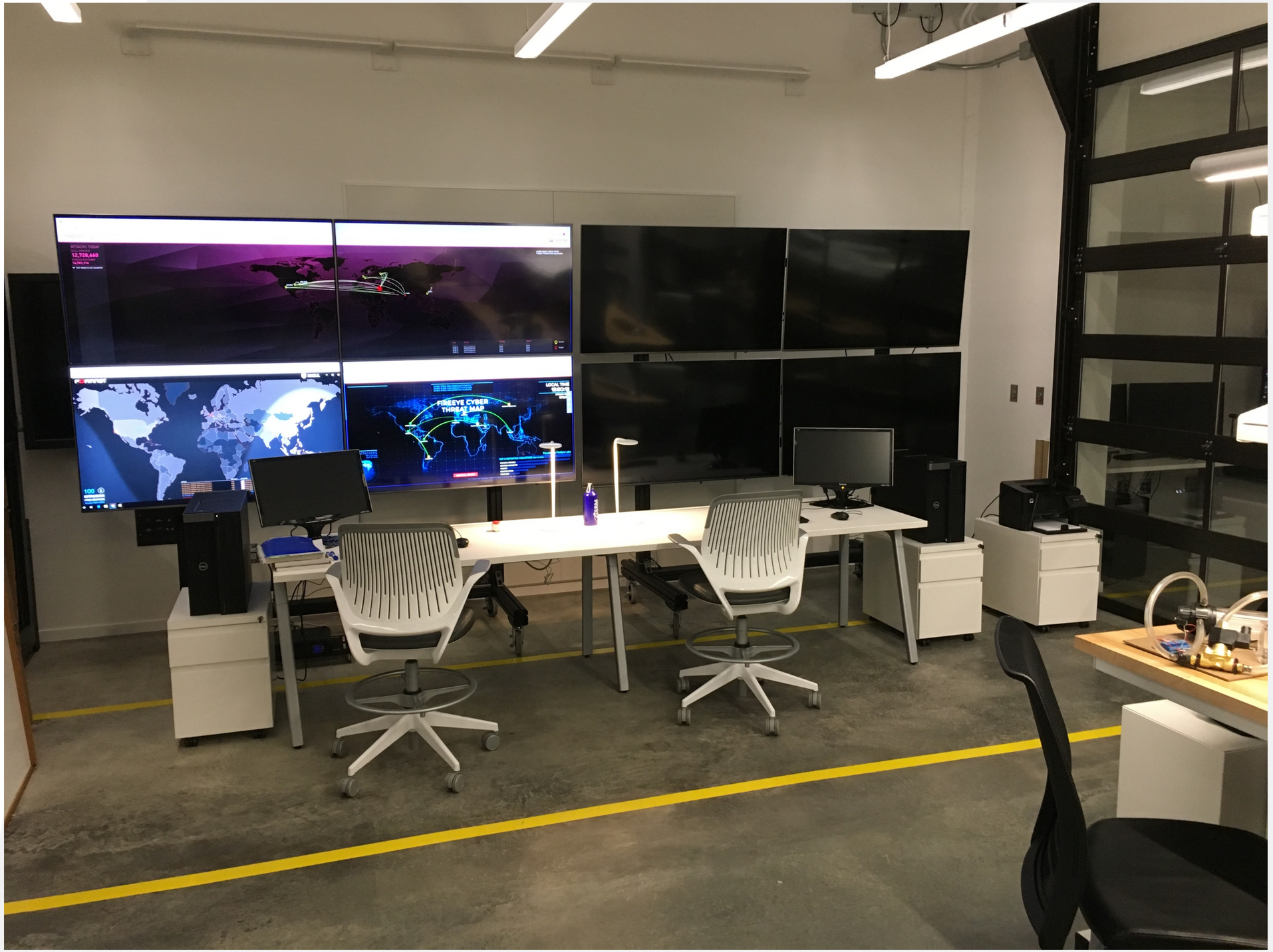
SCADA HMI

Security Analytics



Security Visualization

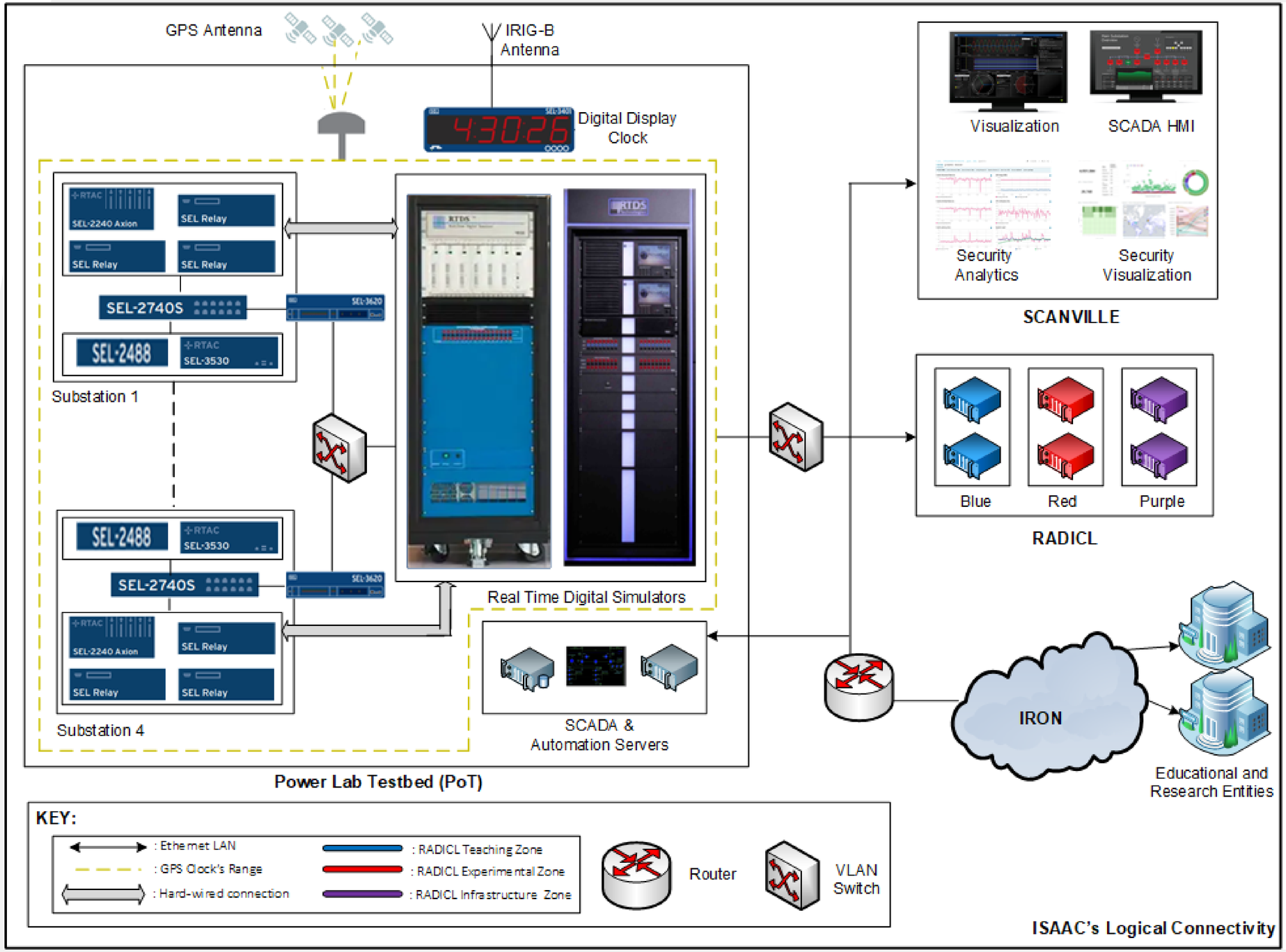
SCANVILLE


FIREEYE CYBER
THREAT MAP

SECURITY CONSIDERATIONS

- Testbed airgap and isolation
- Security policies and procedure
- Virtualization technologies
- Node re-imaging
- Network encryption using MACSec
- Planned security assessment

ISAAC: OVERALL ARCHITECTURE

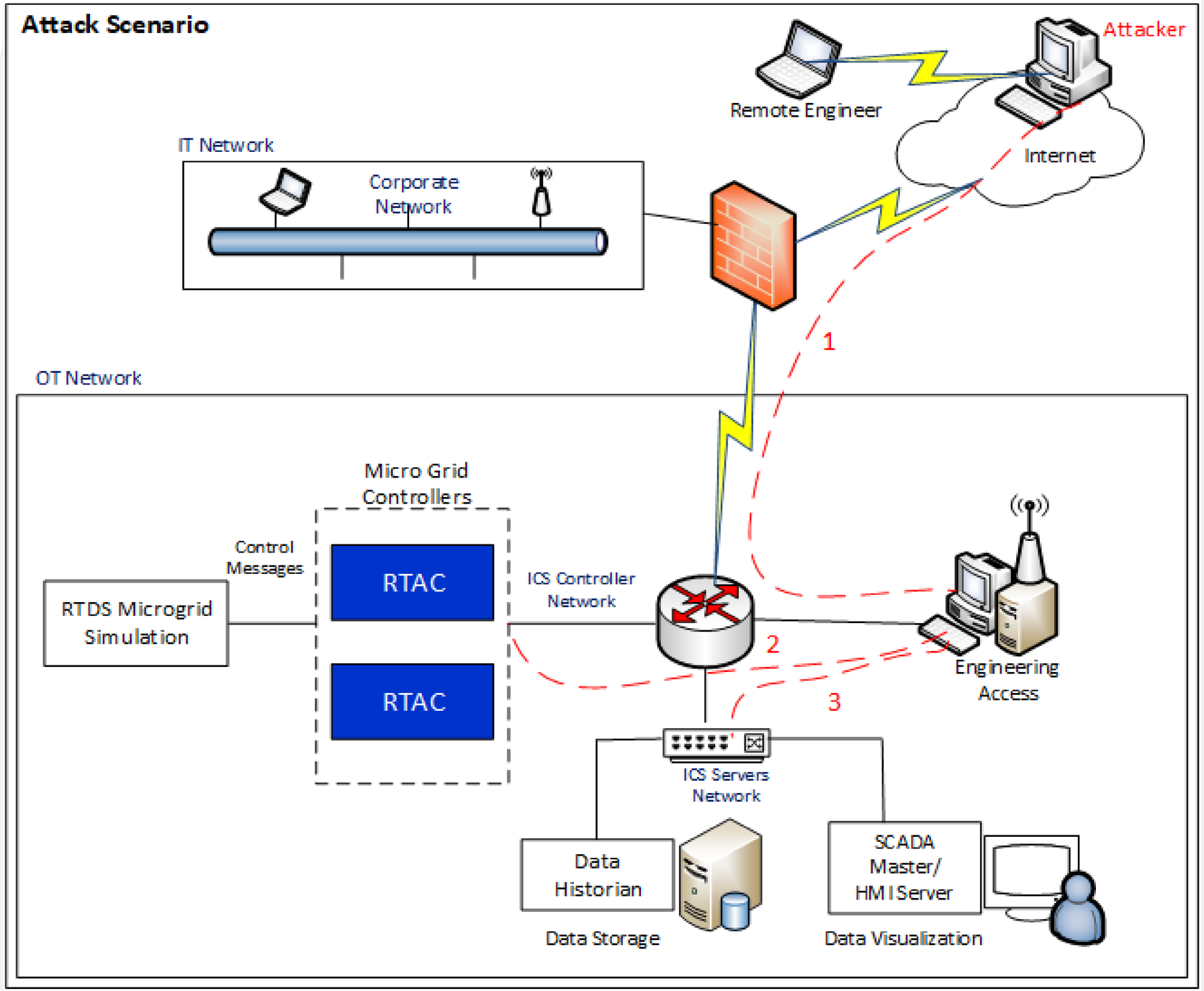


CURRENT PROGRESS

PROGRESS IN PROJECT ISAAC

- Power lab testbed is fully implemented.
- SCANVILLE and RADICL are also fully functional.
- Some current projects:
  - **Resiliency and risk assessment of CPS**
  - Detection of stealth attacks against state estimation
  - Machine learning based situational awareness.

EXAMPLE ISAAC VULNERABILITY ASSESSMENT



EXAMPLE VULNERABILITY ASSESSMENT

- Network reconnaissance.
  - Helps in understanding the network topology.
  - Replay attacks from captured packets.
- Address Resolution Protocol (ARP) poisoning.
  - Man-in-the-middle attack.
  - Network compromised with false data measurements.

FUTURE WORK

NOT SO FUTURE…(ONGOING)

- Integration to University of Idaho facilities in Idaho Falls and Coeur d’Alene using Idaho Regional Optical Network (IRON).

- Further policy and process development

ACKNOWLEDGMENTS

THANK YOU

- State of Idaho via IGEM grant
- NSF Funding via grant number 1565572
- M.J. Murdock Charitable Trust
- University of Idaho IT staff
- University of Idaho Admin staff

THANK YOU!

QUESTIONS & FEEDBACK

- Glad to collaborate
  - Yacine Chakhchoukh (yacinec@uidaho.edu)
  - Brian Johnson (bjohnson@uidaho.edu)
  - Daniel Conte de Leon (dcontedeleon@uidaho.edu)