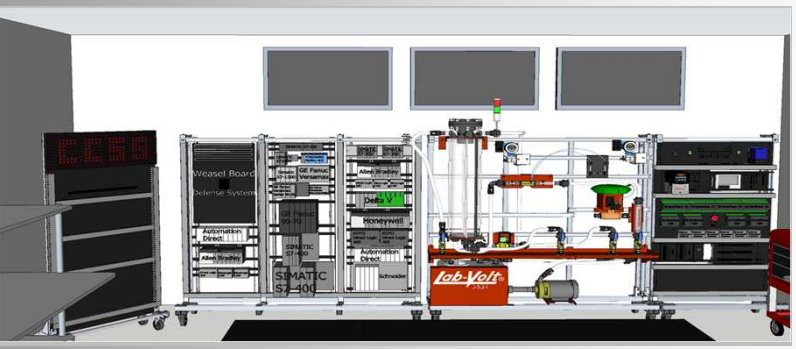
SAND2016-7270PE

*Exceptional service in the national interest*

Sandia National Laboratories




# Sandia National Laboratories Industrial Control Systems (ICS) Security

Jay Johnson and Shawn Taylor

U.S. DEPARTMENT OF ENERGY | National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

# Sandia's Control System Security Research

Sandia National Laboratories

## Provide decision makers with actionable information

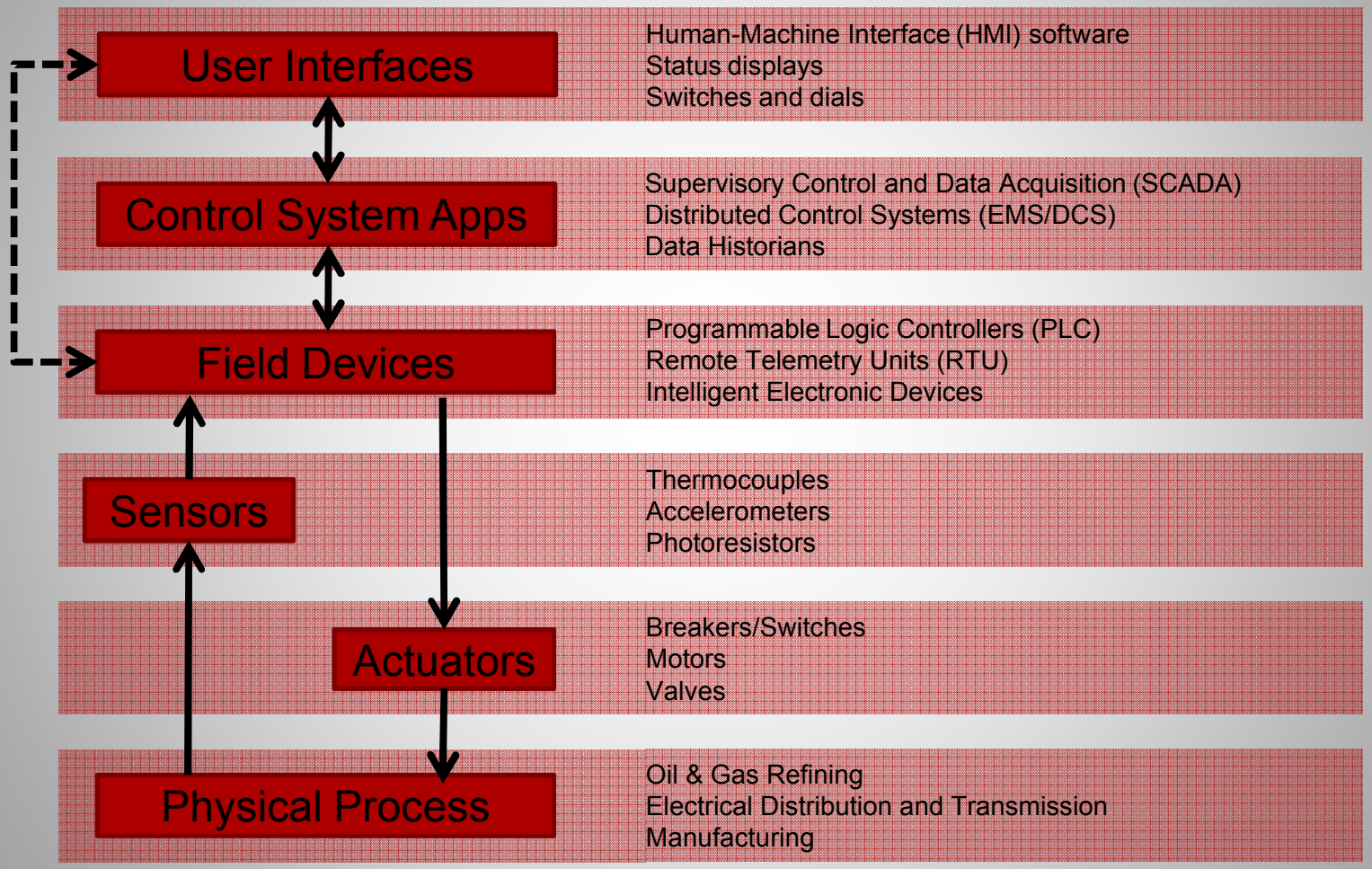
- Red Team Assessments
- Field Device Analysis
  - PLC monitoring and forensics
  - PLC firmware forensics
  - ICS network detection for ICS traffic
- Emulytics
- Exercise/Test Bed support

## Design resilient systems to withstand cyber-attacks

- Research next generation security solutions
- Partner with industry to "push" solutions to market

**Mission:** To reduce the risk of critical infrastructure disruptions due to cyber attacks on control systems.

# Control System Architecture



# Field Device Analysis

Sandia National Laboratories

**Problem**: Field devices are not inspectable

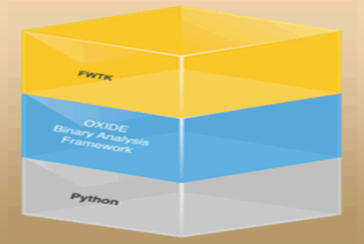
**Solution**: Develop tools and techniques to identify malicious modification

# Analysis Tools

Sandia National Laboratories

## WeaselBoard

Dynamic monitoring between components within a field device




## Firmware Toolkit

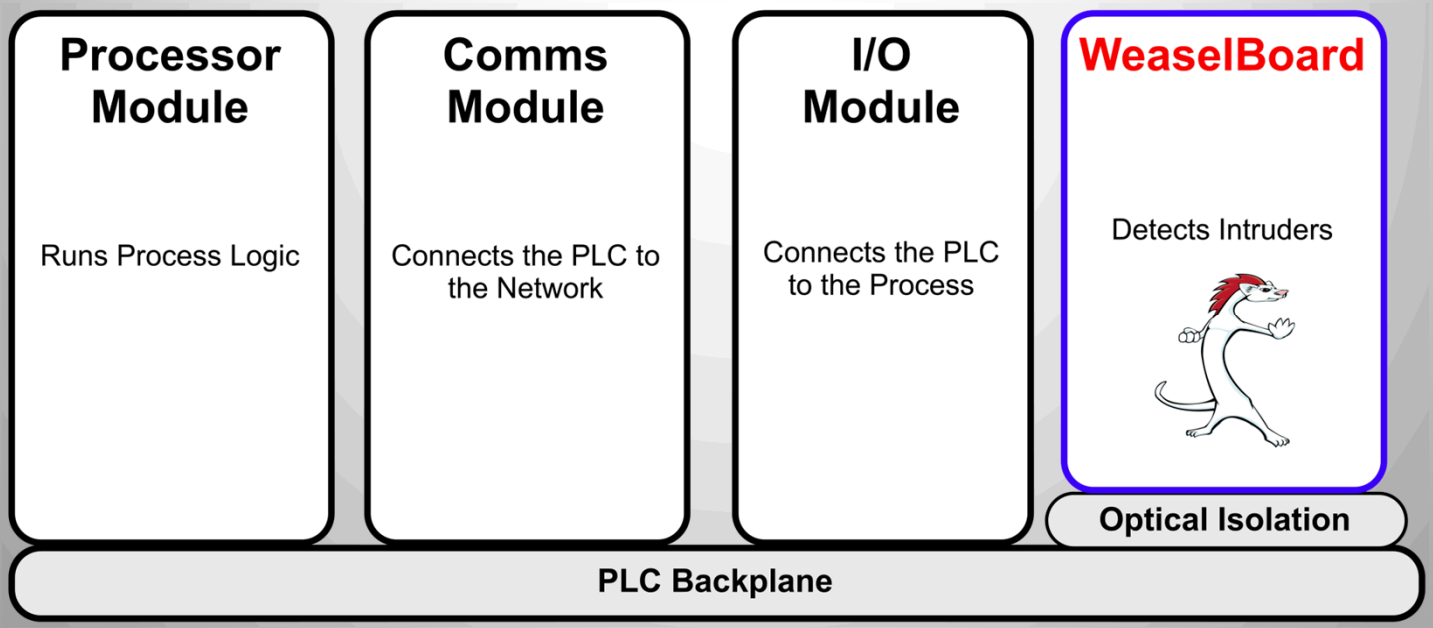
Static analysis of firmware running on a field device

## BroBounds

Dynamic monitoring between field devices

# WeaselBoard

- WeaselBoard connects to PLC backplanes to capture traffic between modules.
- WeaselBoard alerts operators to malicious PLC behavior.
- WeaselBoard can spot:
  - process control settings
  - sensor values
  - module configuration information
  - firmware updates
  - process control program updates



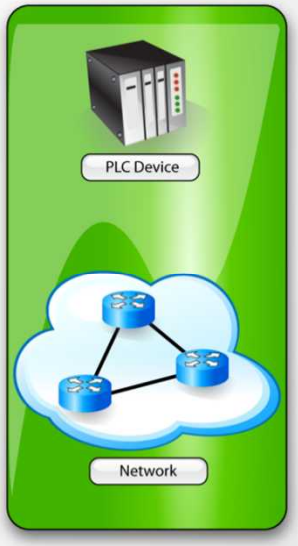
# SCEPTRE – ICS Emulation and Simulation

Sandia National Laboratories

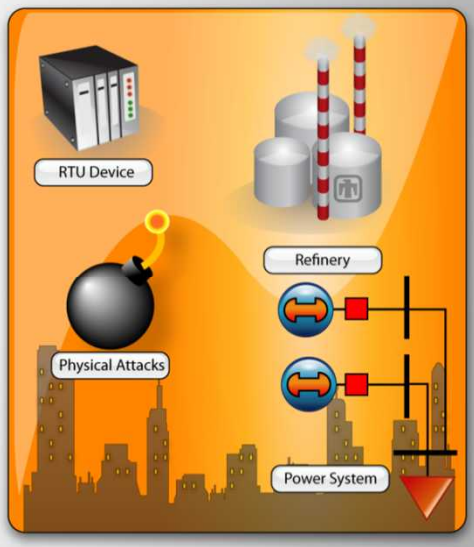
## Human


## Live


## Virtual



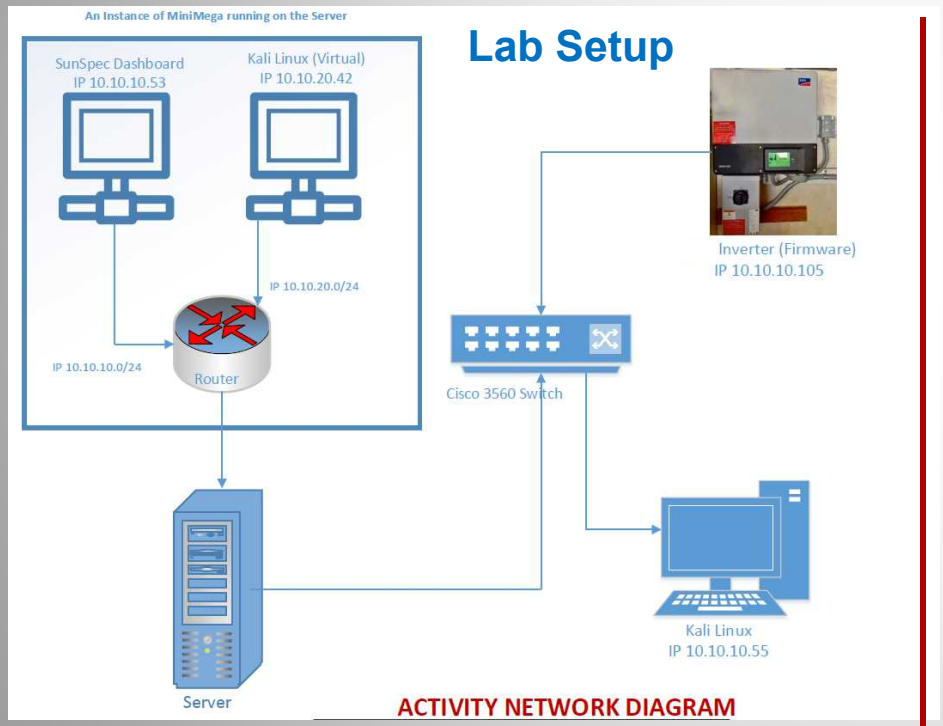

## Constructive



# Cyber Vulnerability Assessment of PV Inverter using Kali Linux

Sandia National Laboratories

- Evaluate security of aggregator/utility to inverter Modbus TCP/IP protocol
- Results can advise the solar industry on weaknesses of control system protocols and offer suggestions



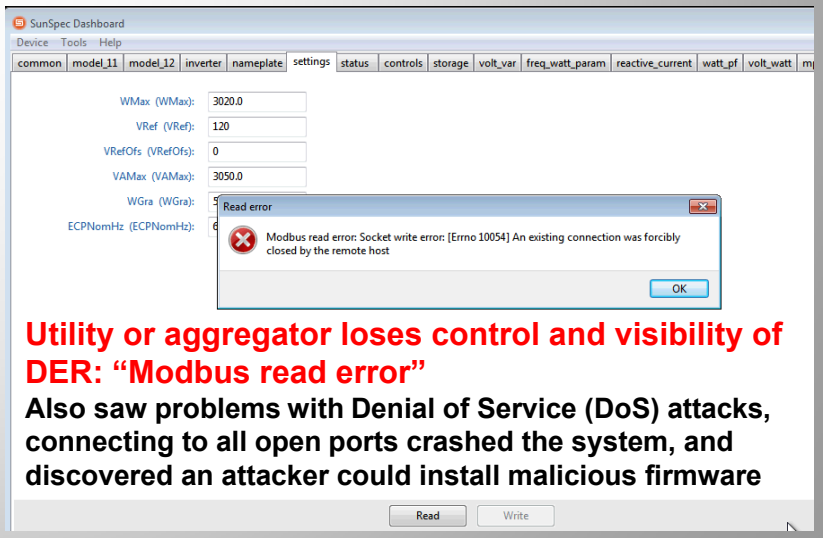

**System:** Physical and virtual machines running Kali
**Vulnerability Assessment:** nmap, hping, OpenVAS
**Penetration testing:** ettercap, metasploit

## Results

Identified Modbus device with port scanning

```
PORT    STATE SERVICE
502/tcp open  asa-appl-proto
MAC Address: 00:40:AD:91:9E:B4 (SMA Regelsysteme Gmbh)
```

Disrupted master (client) –slave (server) communication via Flooding Attack

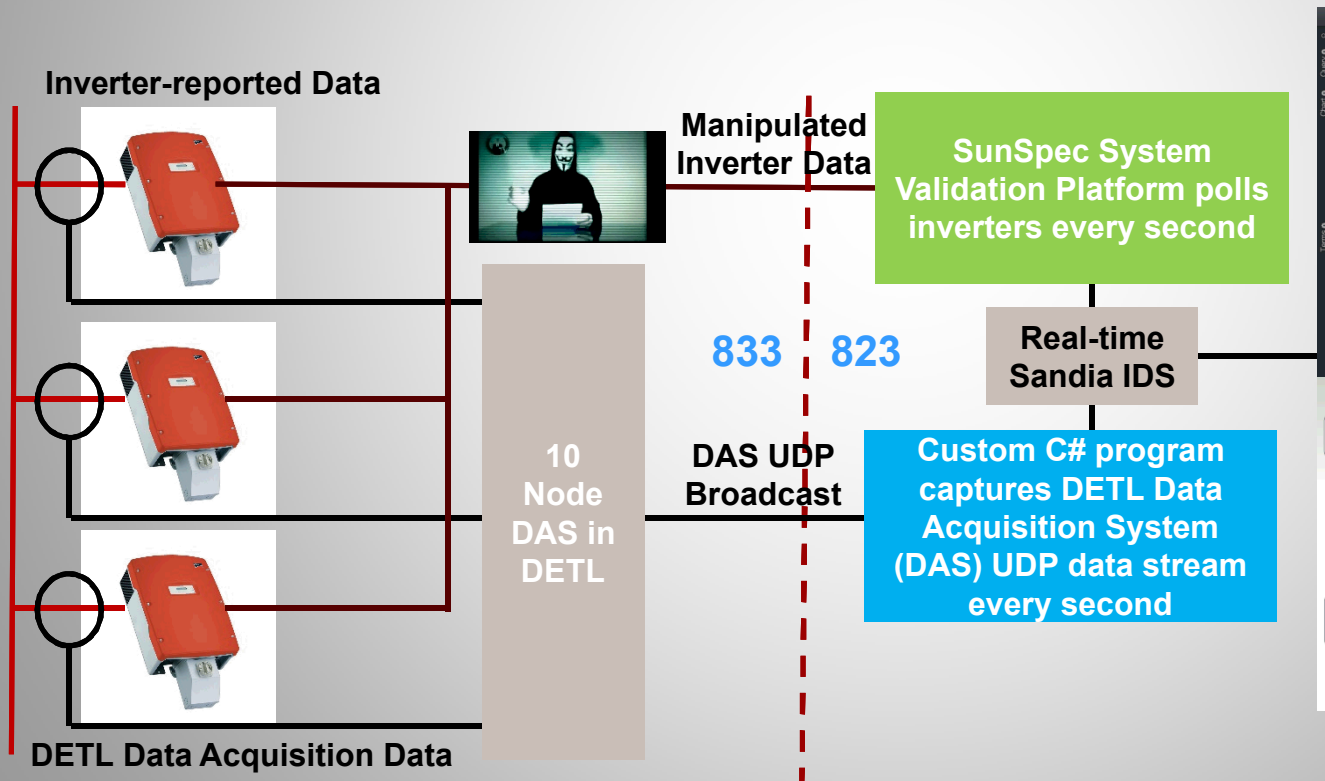


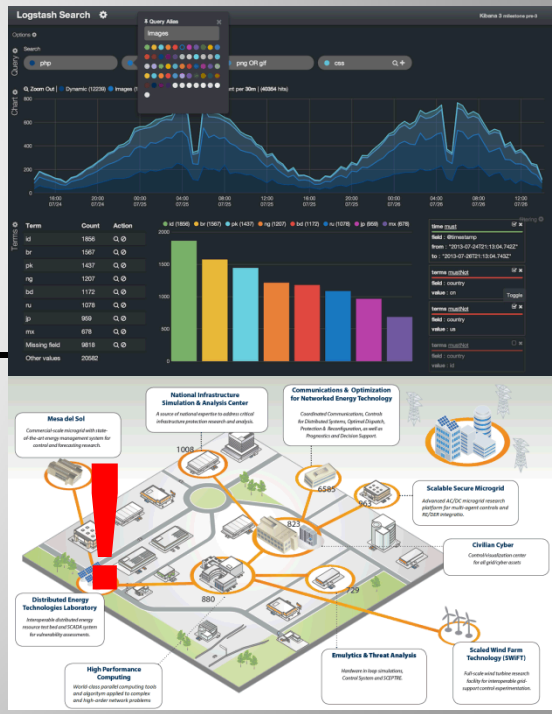

**Utility or aggregator loses control and visibility of DER: "Modbus read error"**

**Also saw problems with Denial of Service (DoS) attacks, connecting to all open ports crashed the system, and discovered an attacker could install malicious firmware**

# Intrusion Detection System Design

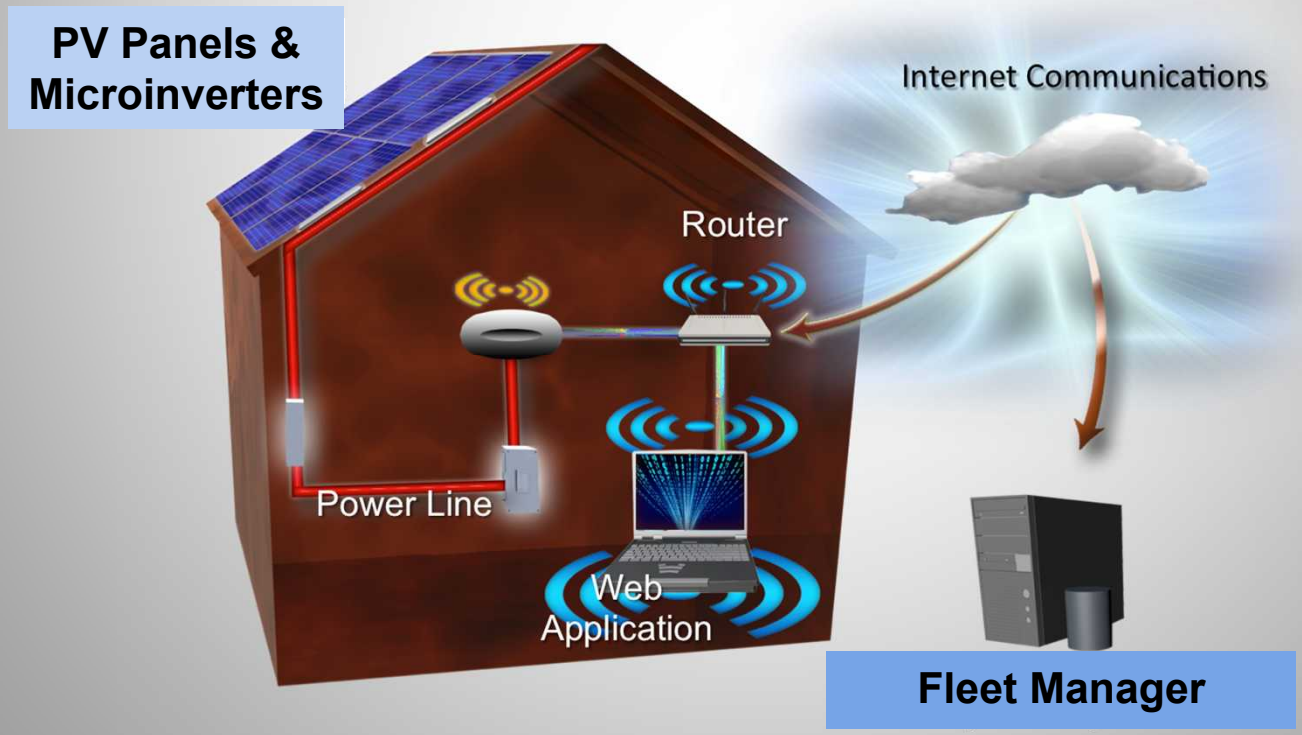
- Data collected from inverters (in-band monitoring) and data acquisition system (out-of-band monitoring, e.g., AMI) sent to 823 for analysis
- Creating real-time intrusion detection systems (IDS) to alarm when inverter data is being falsified or manipulated.



# SNL Cyber Analysis of DER Network

- Working with PV installer in the US with 330,000 fielded end devices.
  - All of them have communications – and soon controls capabilities.
  - Value to partner was review of cybersecurity approach and suggested improvements.
  - Value to Sandia was knowledge of operational renewable resource system architecture.



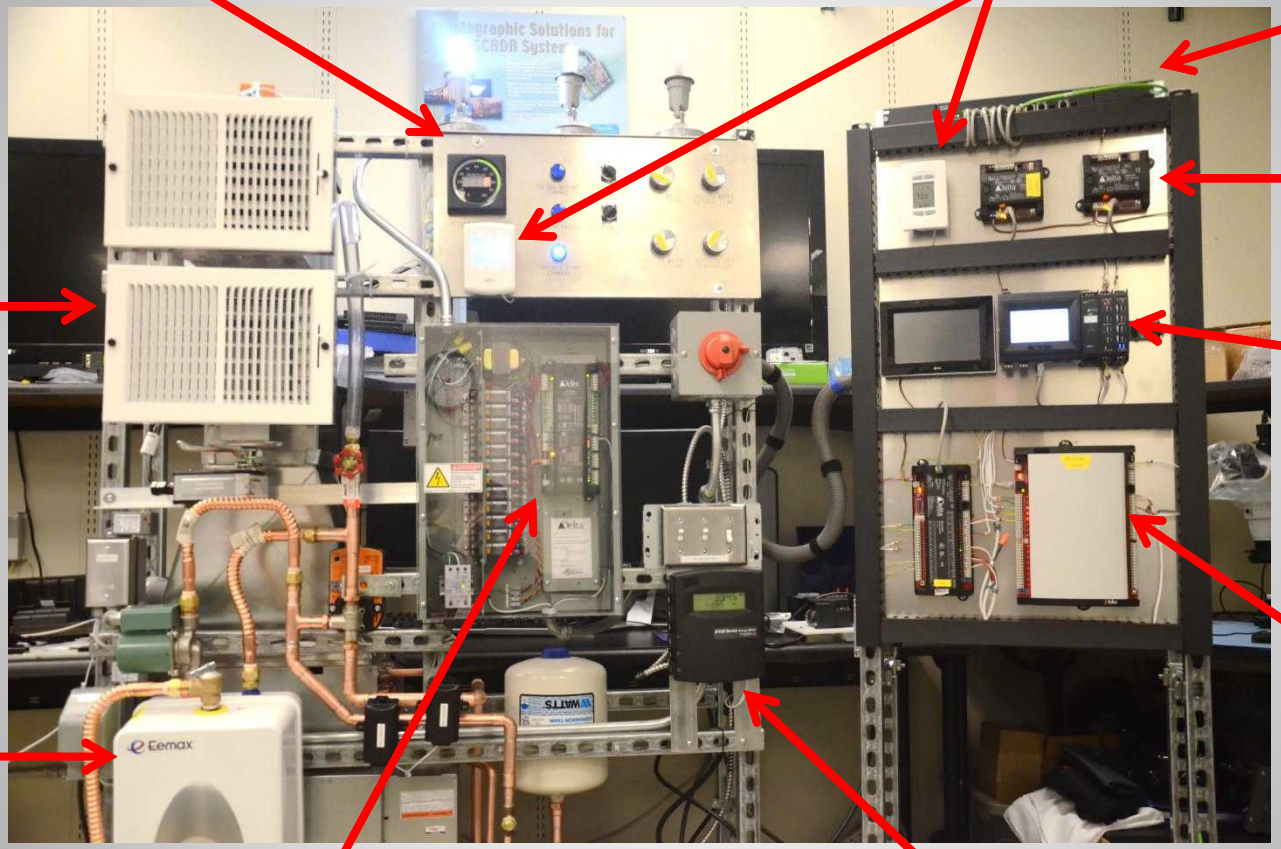
# Sandia Building Automation Test System

Sandia National Laboratories

Chiller (hardware-in-loop emulation)

Thermostats & Room Sensors

Cisco Switch




BACnet & MODBUS routers

HVAC (2 zone)

Expandable Controller module

DSC Controllers

Boiler/HW

Lighting controller (3 zone)

Energy Meter (serial network)

**Allows us to test real-time behavior of system**