SAND2016-7305C

Exceptional service in the national interest

Sandia
National
Laboratories

Cyber Security R&D for Control Systems

Panel Session I: Cyber Security of ICS

Jason Stamp, Ph.D.

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

NNSA 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. 2016-0000P.

Sandia's Control System Security Research

Provide decision makers with actionable information

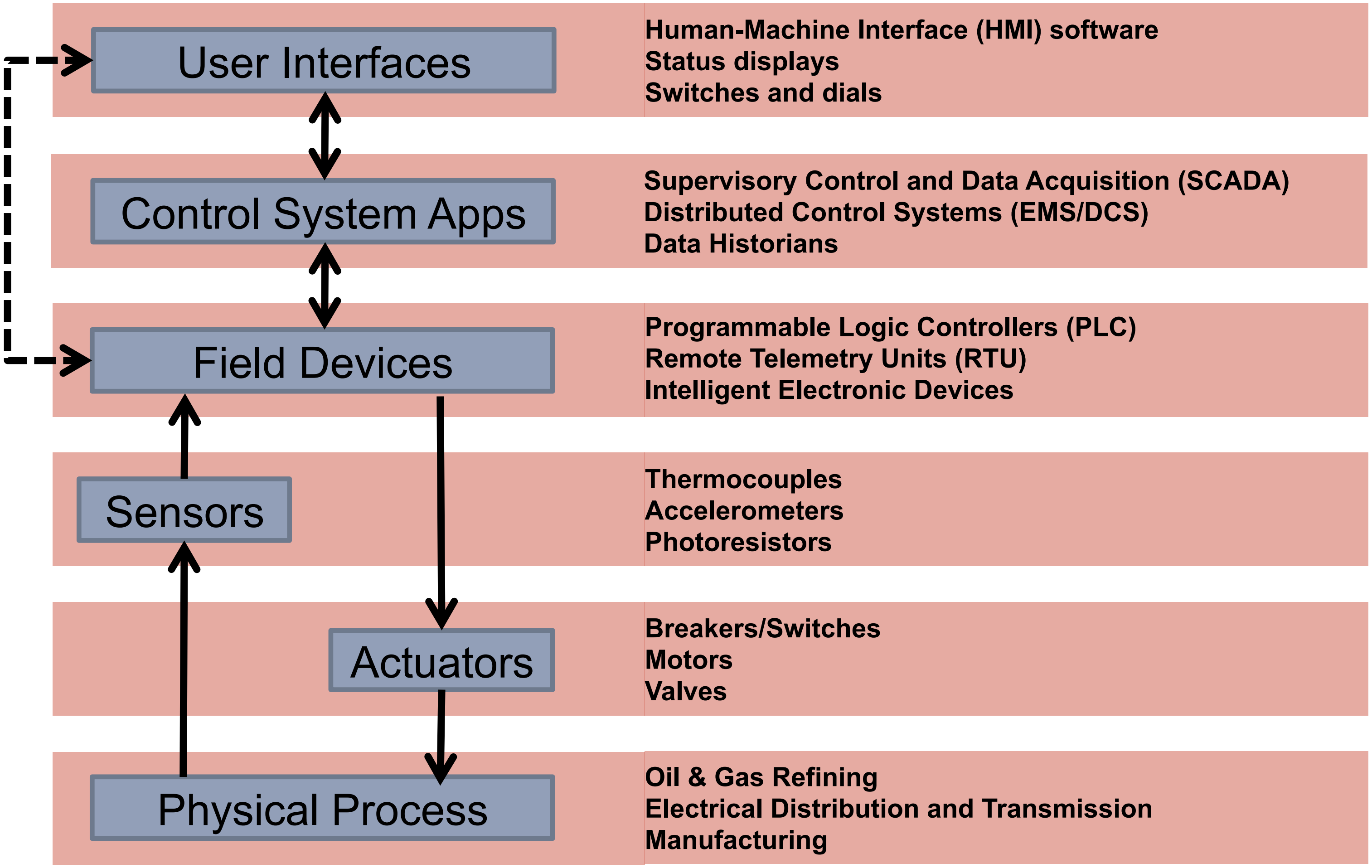
- Red Team Assessments
- Field Device Analysis
  - PLC monitoring and forensics
  - PLC firmware forensics
  - ICS network detection for ICS traffic
- Emulytics (SCEPTRE)
- Exercise/Test Bed support

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



User Interfaces

Human-Machine Interface (HMI) software
Status displays
Switches and dials

Control System Apps

Supervisory Control and Data Acquisition (SCADA)
Distributed Control Systems (EMS/DCS)
Data Historians

Field Devices

Programmable Logic Controllers (PLC)
Remote Telemetry Units (RTU)
Intelligent Electronic Devices

Sensors

Thermocouples
Accelerometers
Photoresistors

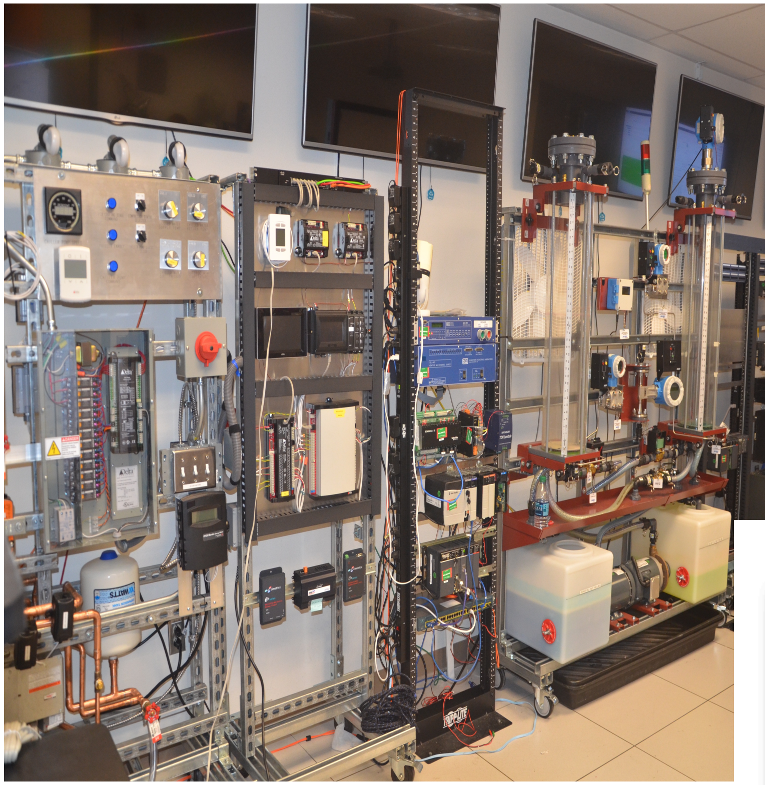
Actuators

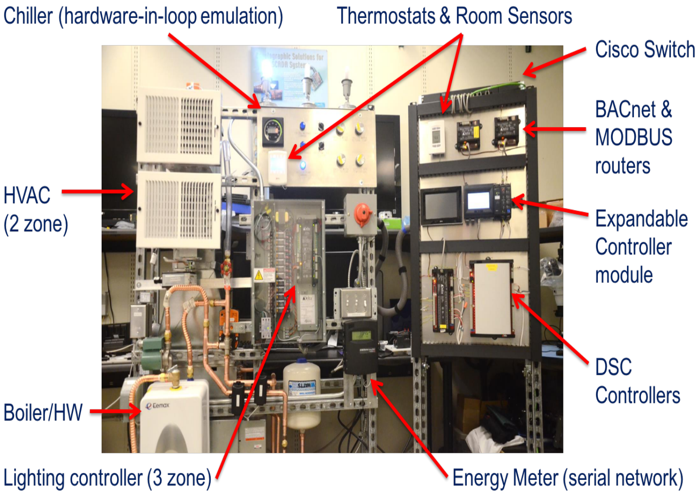
Breakers/Switches
Motors
Valves

Physical Process

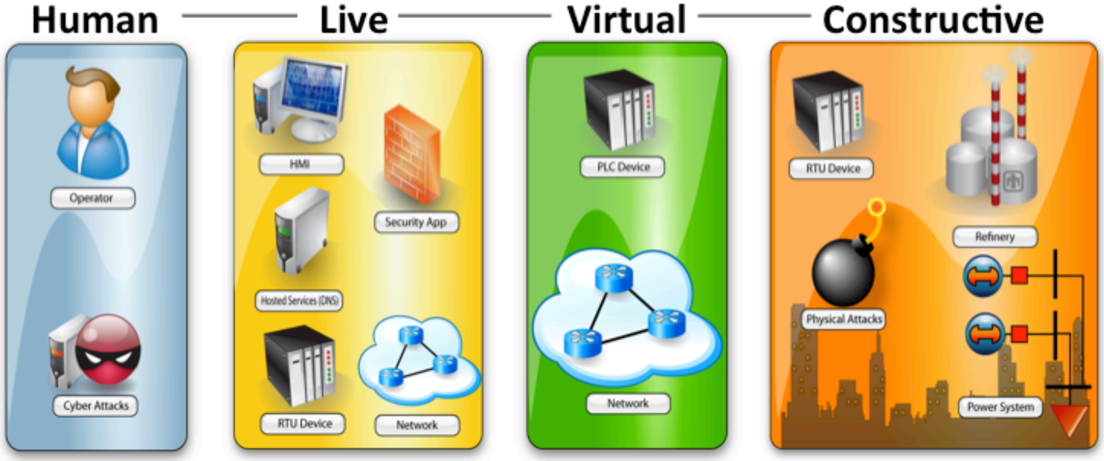
Oil & Gas Refining
Electrical Distribution and Transmission
Manufacturing

Representative ICS Testing Environments




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)

Emulytics™/SCEPTRE

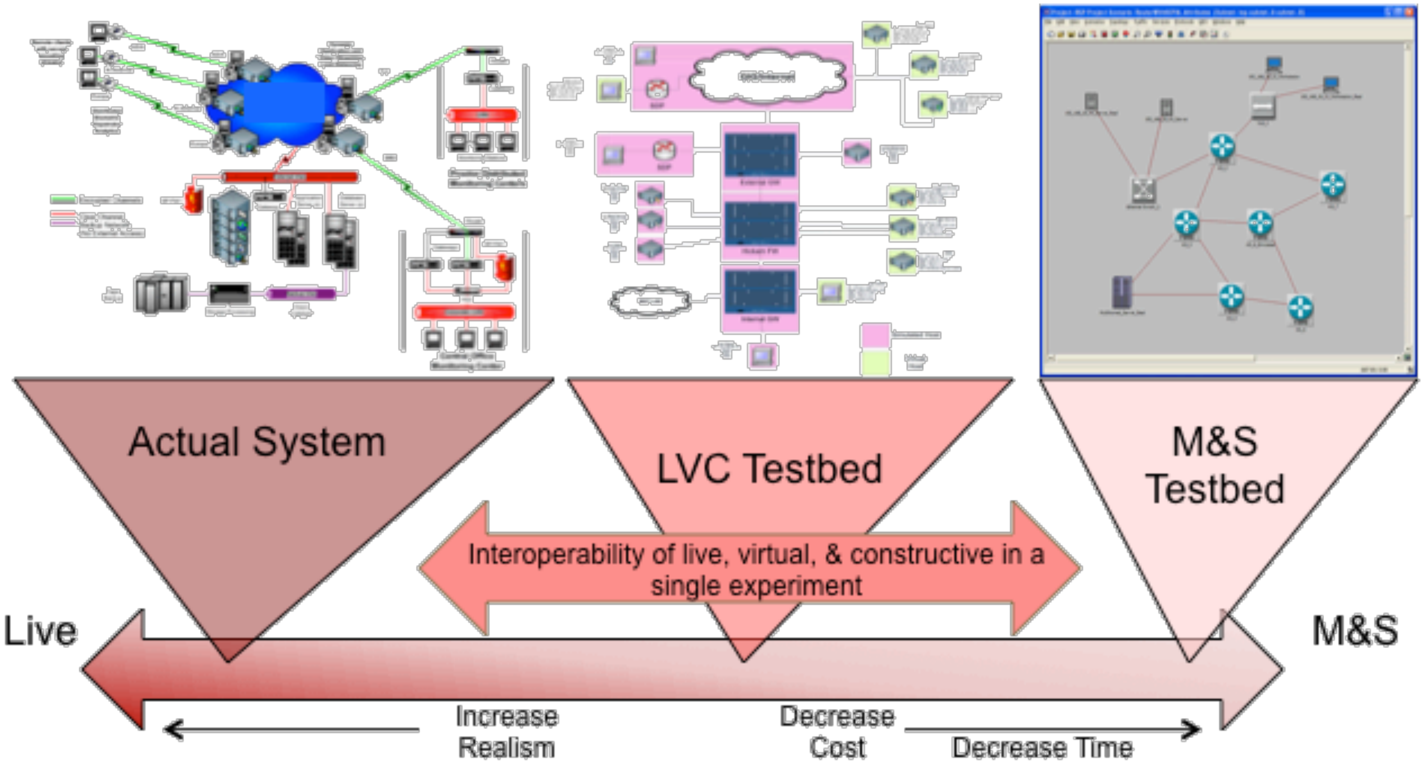


SCEPTRE Operational Overview

- SCEPTRE provides a cyber-physical environment to show interaction between cyber-initiated events and the physical world
- Balances need for M&S accuracy against testing resources
  - Live system testing: potential damage to the real system and dangers to human life
  - Test bed systems: Expensive to build, maintain, configure, and operate
  - Labscale hardware testing setups: May require the context of a larger, networked system
- Devices (simulated, emulated, real) communicate/interact via ICS protocols
- All ICS devices are able to interact with the process simulation, providing both updates and subscribing to the current state of the simulation
- Overall simulation is able to bridge multiple infrastructures into the same experiment to show interdependencies
- Use cases:
  - Test and evaluation
  - Mission rehearsal
  - Other analysis: understand vulnerabilities and exploitable avenues, identify critical components on the control network, model infrastructure interdependencies, etc.

SCEPTRE Cyber Security Analysis for ICS

- Control systems devices: simulated RTUs, PLCs, relays; emulated PLCs, FEPs, HMI services; real HITL relays, PLCs, RTUs
- High fidelity SCADA protocols: ModbusTCP, DNP3, IEC61850
- Process simulation: industry standard software where possible, PowerWorld, PyPower, PSSE for electricity, water treatment, refining, oil/gas pipelines



Actual System

LVC Testbed

M&S Testbed

Interoperability of live, virtual, & constructive in a single experiment

Live

M&S

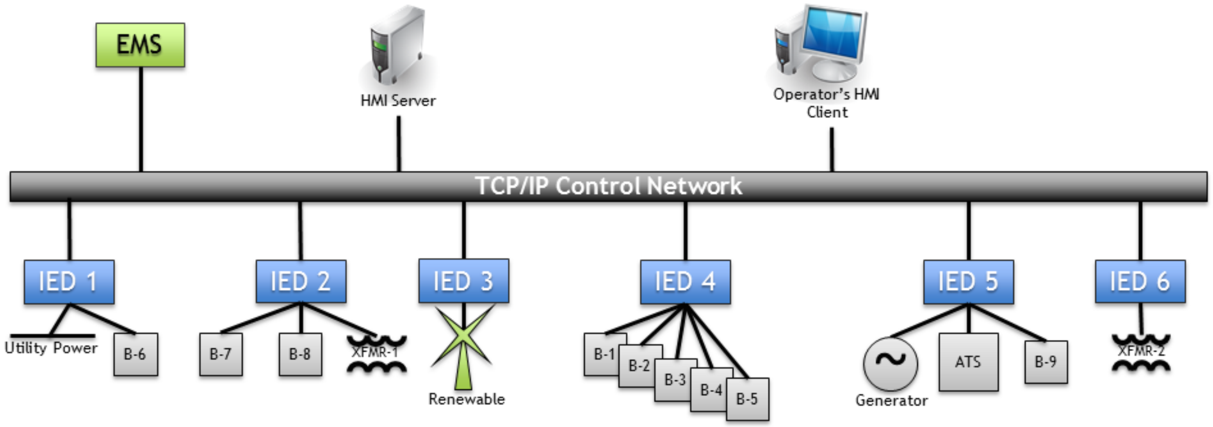
Increase Realism

Decrease Cost

Decrease Time

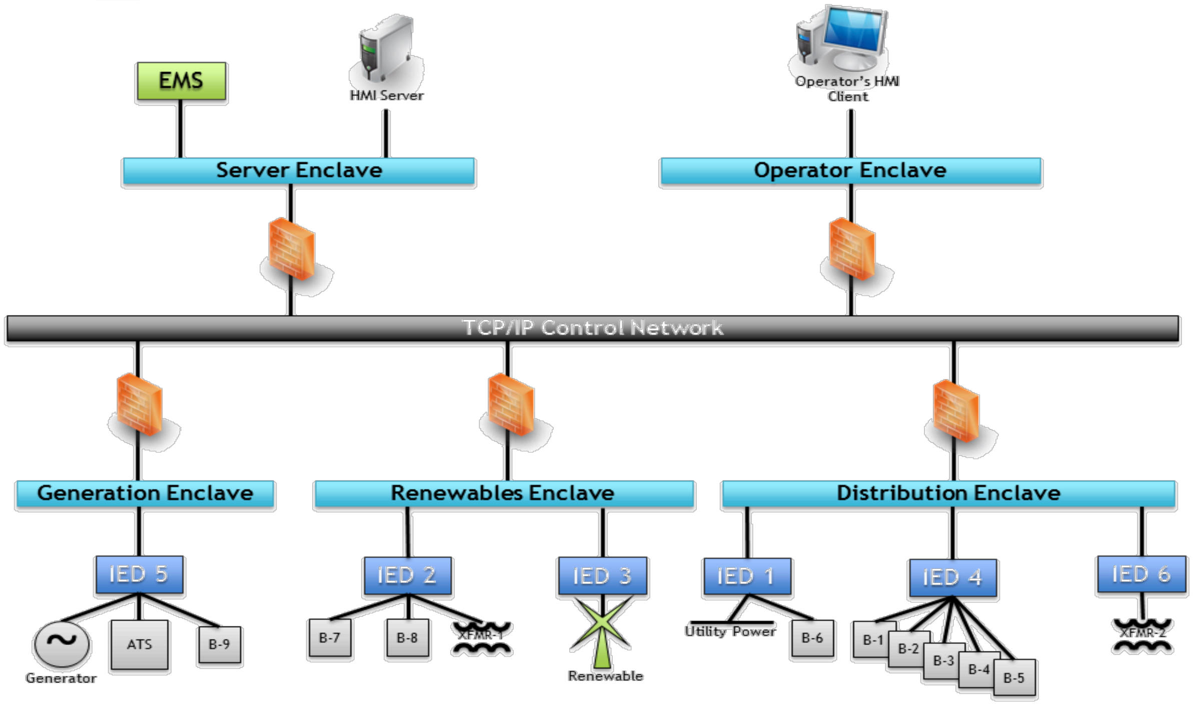
Defense-in-depth: Application of Enclaves and Functional Domains

Sandia National Laboratories



Flat

Segmented



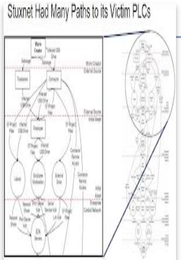
Advanced Field Device Monitoring

PLCs are vulnerable to targeted attacks that cost millions in equipment damage, lost operation, or injured personnel.

PLCs are not monitored for security compromise.

It is not enough to build “secure” products. The ability to inspect and detect is necessary for systems that will be in place for decades.

A backplane analysis system examines the communication between PLC modules



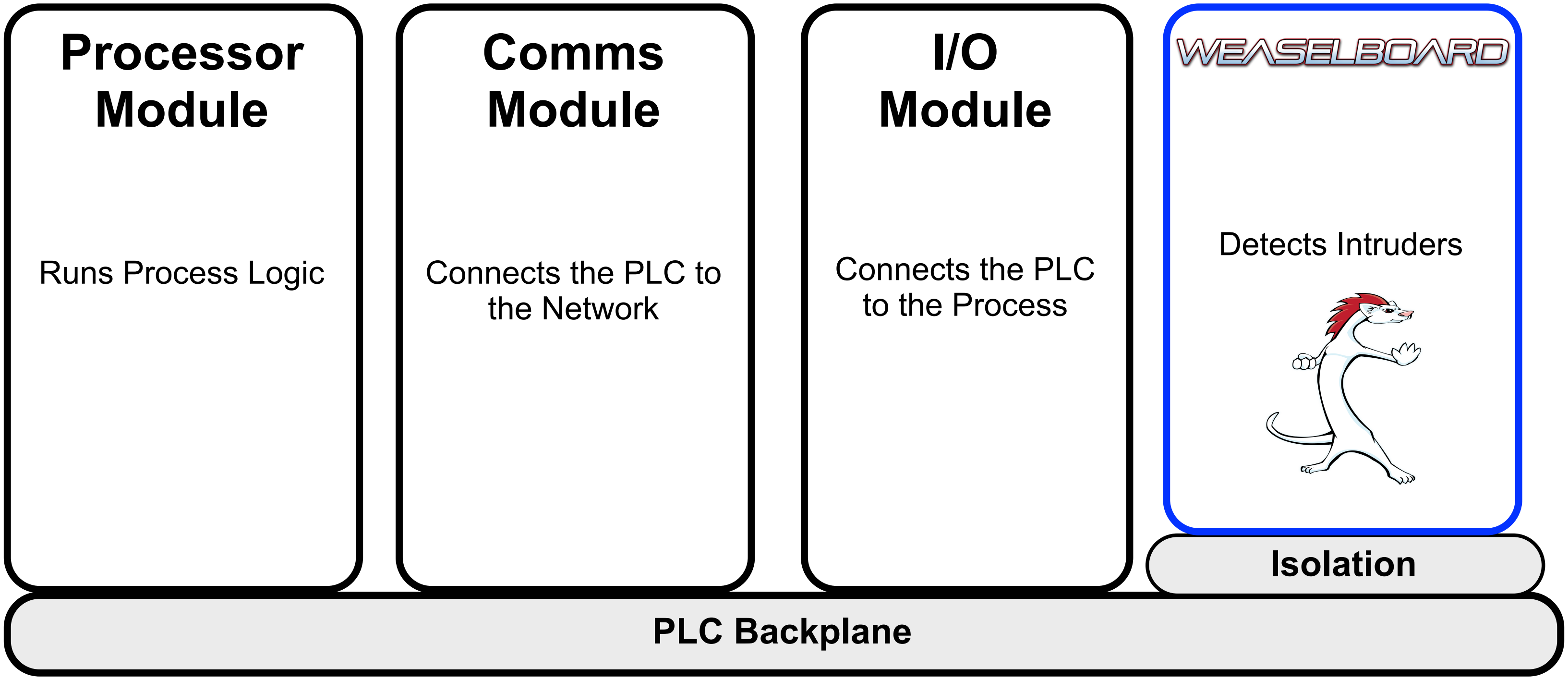
Cyber attacks on the control systems will result in anomalies visible on the PLC backplane.

New Capabilities for PLCs:

- Forensics: After compromises, detect modifications to hardware, firmware, or logic
- Detection: Actively detect anomalies

Network monitoring alone is not sufficient to adequately defend against a sophisticated adversary

Advanced Field Device Monitoring



Processor Module

Runs Process Logic

Comms Module

Connects the PLC to the Network

I/O Module

Connects the PLC to the Process

WEASELBOARD

Detects Intruders

Isolation

PLC Backplane

- WeaselBoard plugs into the backplane and listens to the conversations between control system modules
- There is a lot of granularity in these conversations, which allows WeaselBoard to uniquely observe behavior of the control system independent of the processor and alert when the system is not operating within a specifically defined manner
- Because it alerts on effects of an attack in progress, and not on signatures of prior attacks, WeaselBoard can detect zero-day exploits

General ICS Cyber Security Recommendations

- Investigate all mitigation options, covering defend, detect, and manage (including incident management/recovery plans)
- Develop and install detection capabilities for attack/anomaly indicators
  - Complementary options include network traffic monitoring and advanced hardware monitoring
  - Reduce troubleshooting duration
- Minimize attacker opportunities for device configuration or firmware access (possibly disallowing such network traffic)
- Develop logic- and tamper-checking tools for devices and systems
- Focus on cyber security assessment for field devices