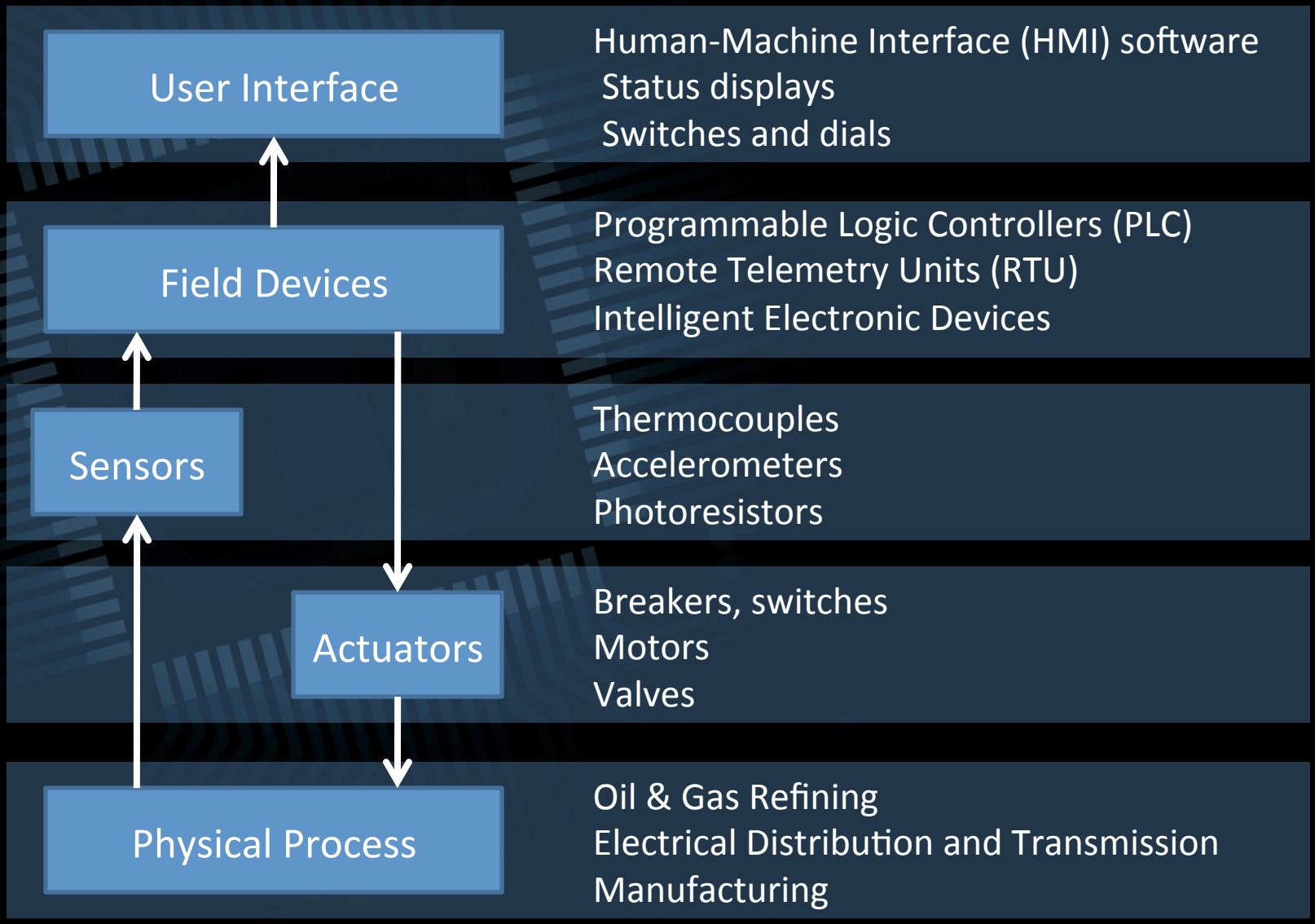
WeaselBoard: A PLC Backplane Analysis System

John Mulder

Sandia National Laboratories

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.

Control System Architecture



Problem

- United States critical infrastructures rely on Programmable Logic Controllers (PLCs) and similar component field devices for many key functions.
- Assessments have made clear that the control systems controlling our national infrastructure deserve more active cyber defense.

Need

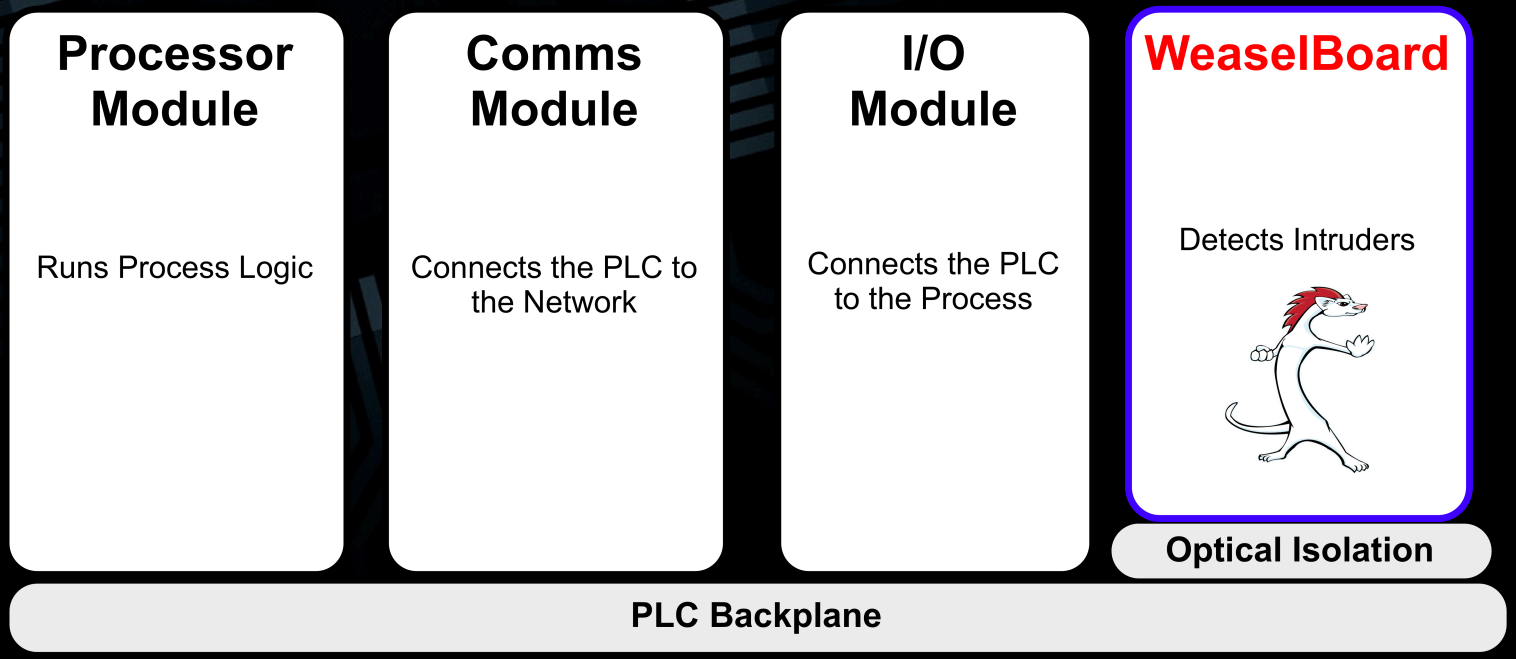
- PLCs are vulnerable to targeted attacks that cost millions in equipment damage, lost operation, or injured personnel.
- PLCs are not monitored for security compromise.
- It is not enough to build “secure” products. The ability to inspect and detect is necessary for systems that will be in place for decades.

Solution: Backplane Analysis System

- 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

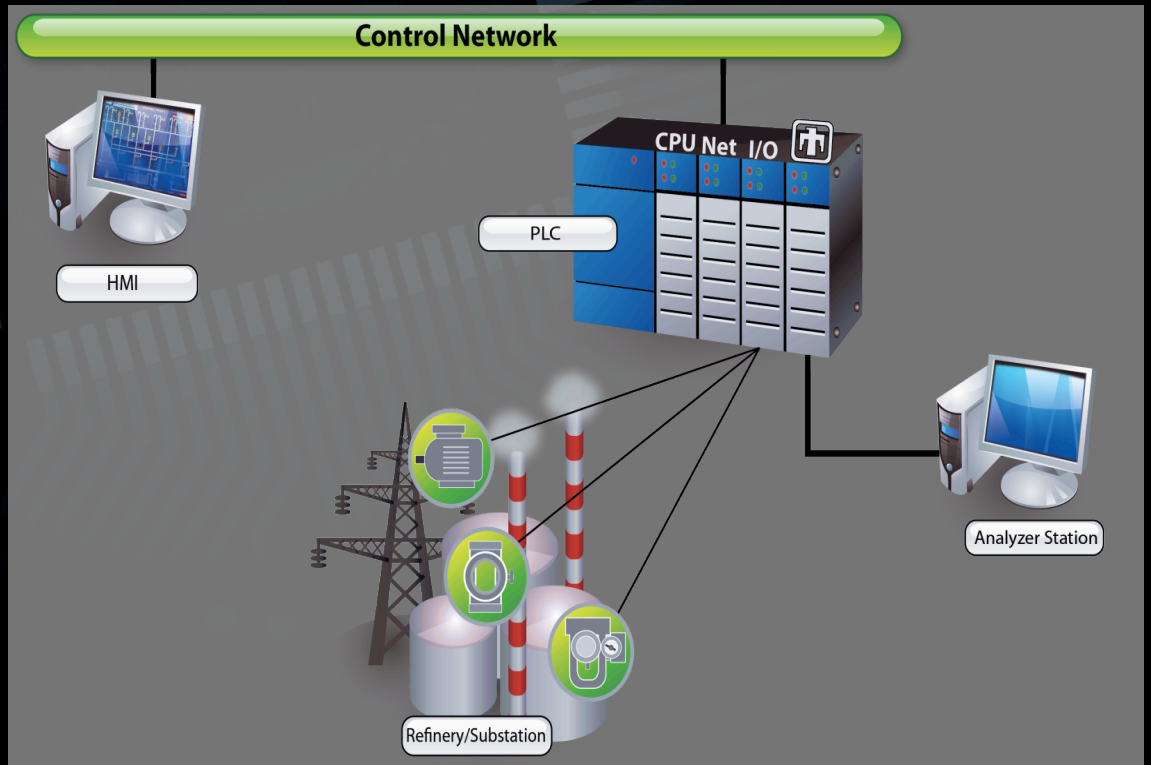
Approach

- WeaselBoard connects to PLC backplanes to capture traffic between modules.
- Alerts operators to malicious PLC behavior



Concept of Operations

- Detects any compromise that effect the process.
- Regardless of the source and location of the attack, WeaselBoard notices the attack's effect.



Things WeaselBoard Can Spot

- process control settings
- sensor values
- module configuration information
- firmware updates
- process control program updates

Current Status: Lab Tested System

- Tested in PLCs:
  - Tested in several different lab systems
  - Validated using control system physical processes
- Hardware:
  - WeaselBoard
  - Adapter board for Allen-Bradley ControlLogix
  - Adapter board for Siemens S7-300
  - Streams raw backplane captures to an analysis workstation
- Analysis Software
  - Can identify large changes to a system (new ladder logic being loaded)
  - Requires a very knowledgeable user

Next Steps

- Government Customer has funded new development
- DHS is funding Transition-to-Practice

Sandia National Laboratories

Industrial Control System Field Device Analysis

John Mulder
jmulder@sandia.gov
Tech Lead

Michael King
making@sandia.gov
Software Lead

Abe Clements
aacleme@sandia.gov
Hardware Lead

Sandia National Laboratories