SAND2018-3532C

Active and Passive ICS Analysis

PRESENTED BY

Jennifer Trasti and Sarah Hostetler

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.

Outline

What is the problem?

How is it solved today?

What is the new approach?

Archimedes

PEAT

WeaselBoard

What is improved by our approach?

Next steps

Limitations

Authentication vs Encryption

What is the problem? Control Systems are Hard to Secure

Damage from messages not inherently “bad” or malformed

Process context required to find a bad actor. (Is it an attack or a lighting strike?)

No way to examine components

- Vendor intellectual property protections
- Vendor-controlled access
- Diversity of standards

Vulnerabilities remain for a long time

Components are not designed for the hostile, interconnected reality

How is it solved today? Adapting IT cybersecurity to OT networks

Signature-based detection

Packet header analysis

Boundary protection

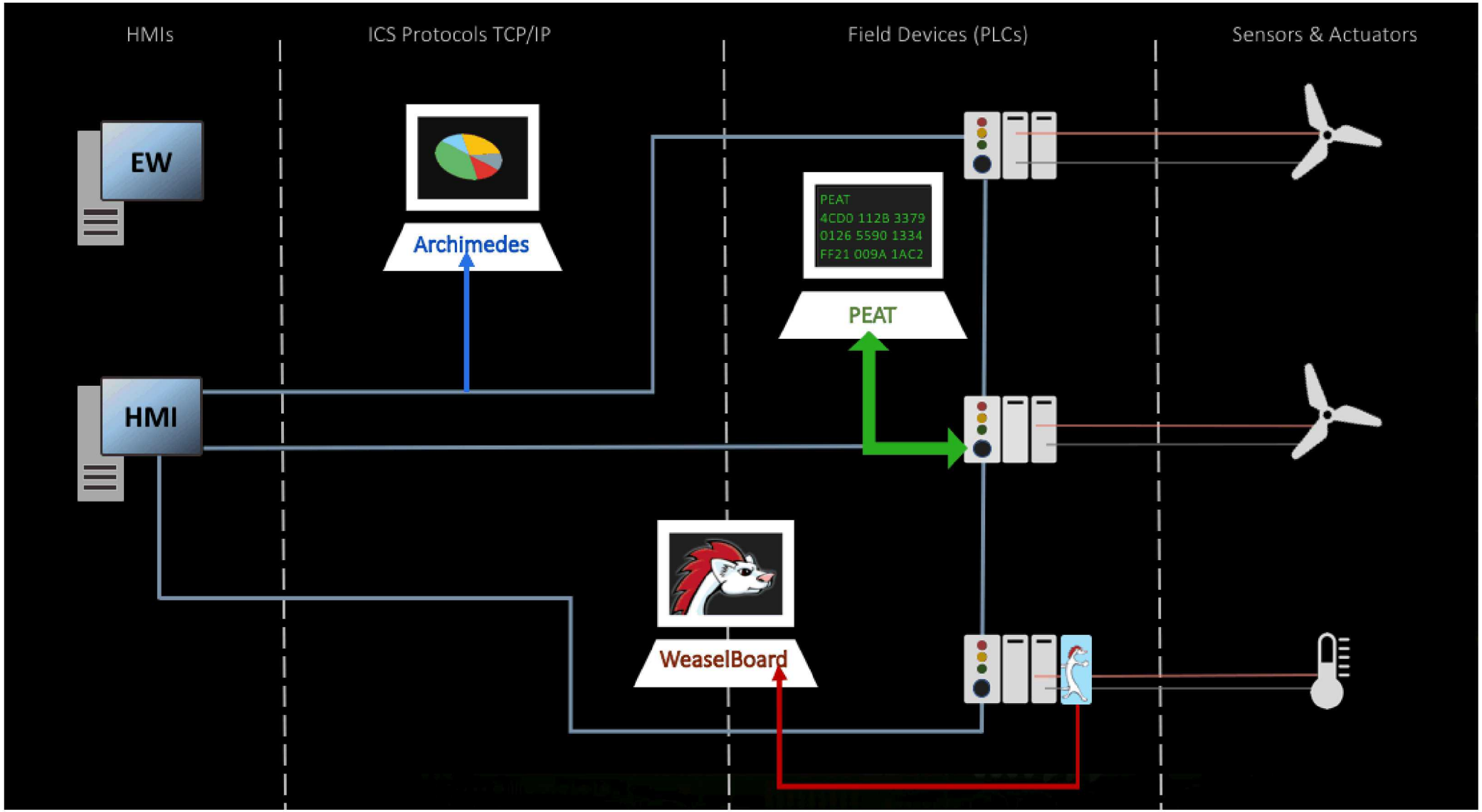
What is the new technical idea? Deep Component Inspection

The VEDAR tools combine active and passive scanning at multiple component layers of the system

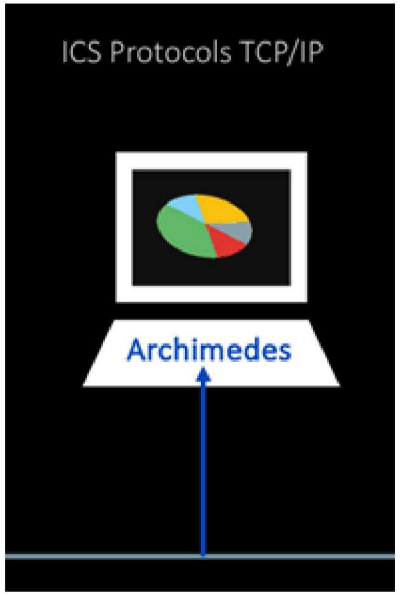
- Control system protocol traffic
- Field device software
- Field device internal communications

VEDAR means “to see, to understand” (in ancient Dalmation)

Multiple Layers of ICS Network Scanning



Protocol Layer: Archimedes Extraction



Pcap/passive live captures of deep-packet data provide

- Real-time visualization of process values out-of-band from HMI
- Forensic examination of process values after an event

Protocol-specific parsing

- Different parser for each protocol

Protocol-agnostic storage

- Elasticsearch database
- Visualization and comparison across vendor/protocol

Dynamic time-series view of the process

Protocol layer: Archimedes Situational Awareness

Visualization of multiple registers

Statistics from register values over time

Relationships between register values

- As temperature increases, so should pressure

Visualize baseline register behaviors

- Processes have regular, repetitive register read/writes

Analysis written in Python to enable changes in the field

Protocol layer: Archimedes Detection

Determine register bounds from sample traffic

- The more diverse the events, the better
- Bounds evolve as more diverse traffic is seen

Visualize anomalous behavior

- Change in message frequency, length, distribution
- New registers queried by the program
- Register bounds exceeded
- Rapid switching of register values (as in Crash Override)

Alert on attacks (research in progress)

- Rule-based
- E.g., set-point originates from OPC server, not from HMI

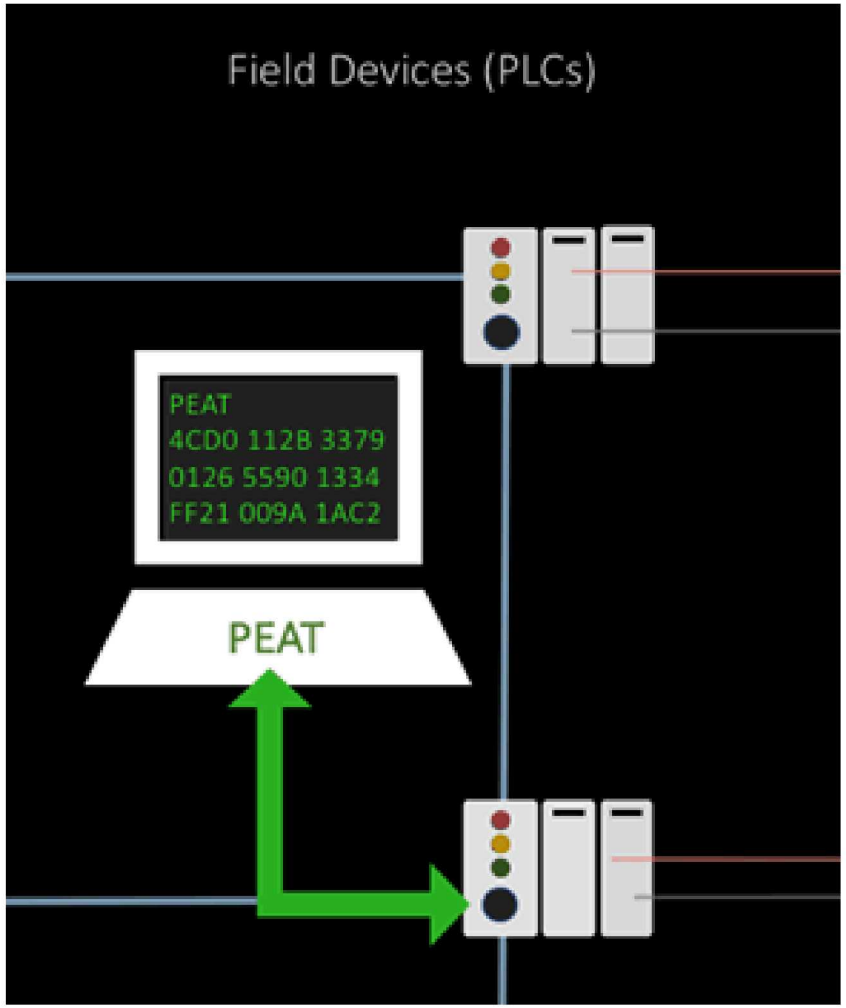
Field Device Software Layer: PEAT Extraction

PEAT = PLC Extraction and Analysis Tool

Scans network for field devices of vendor/model type

Issues device-specific commands to each

Extracts binary data blob(s) from device



Field Device Software Layer: PEAT Analysis

Analyze binary data blob

- Extract Programmable Logic Controller (PLC) programs (process logic code)
- Extract configuration data
  - Network connection information
  - Login attempts
  - Device, model, serno
- Logs

Ladder logic decompiler

- STL-like results
- Device-dependent

Field Device Software Layer: PEAT Detection

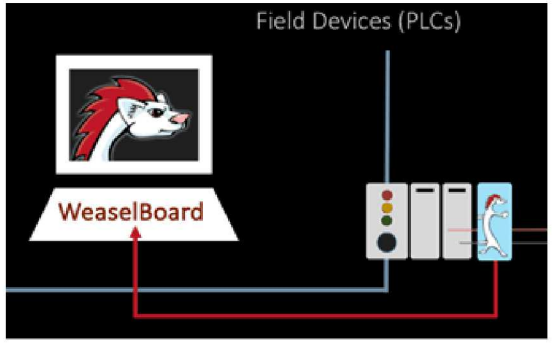
Data compared with a “golden master” copy

- Detect malware or misconfiguration

Examples of discoveries

- Modified process logic (as in Trisis)
- Configuration settings have changed
- Excessive failed access attempts

Field Device Internal Communications: Weaselboard Extraction



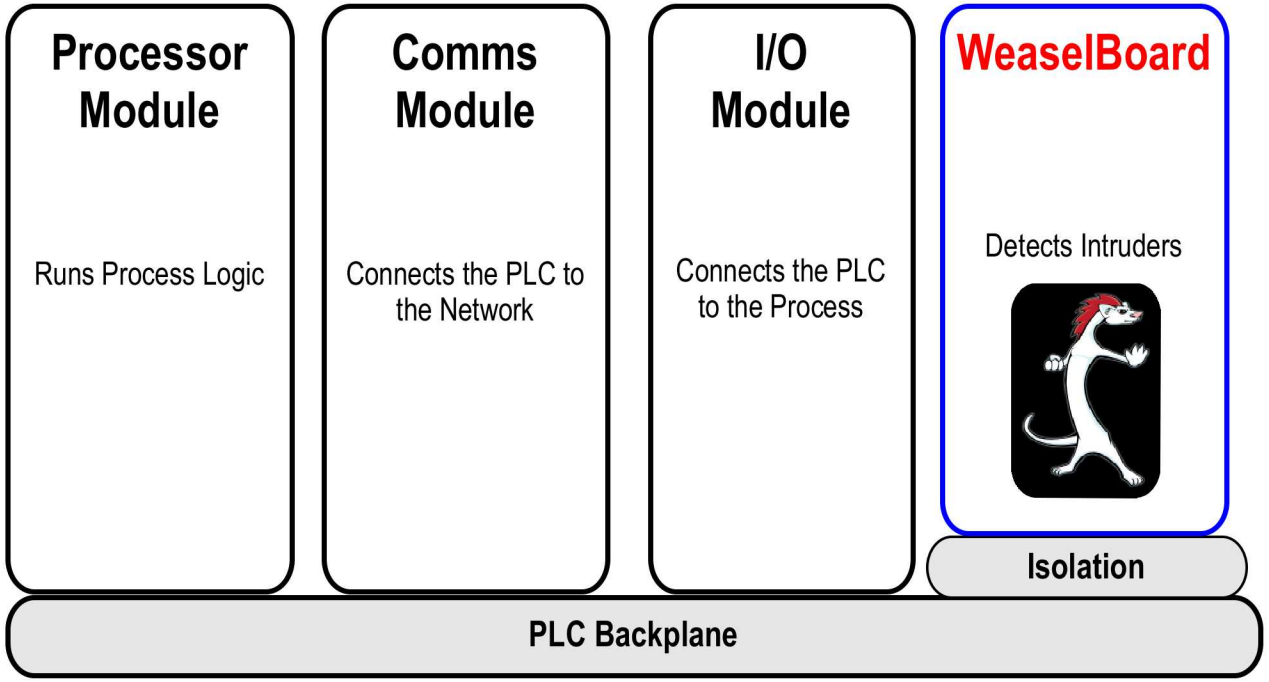
Hardware module that sits in the PLC on the communication bus (backplane)

Listens to all inter-module communication

- Passive, hardware-isolated from writing to the bus

E.g., for many PLCs this means all:

- Messages between network (HMI) and CPU (logic)
- I/O signals from the physical process (to this PLC)
- Communication between CPU and I/O modules
- Vendor backplane protocol traffic
- Vendor or customer-specific protocol traffic



Field Device Internal Communications: Weaselboard Analysis

WeaselBoard rules engine accepts system-specific conditions

- In json form

rotation > 2500 rpm then temperature > 1500F

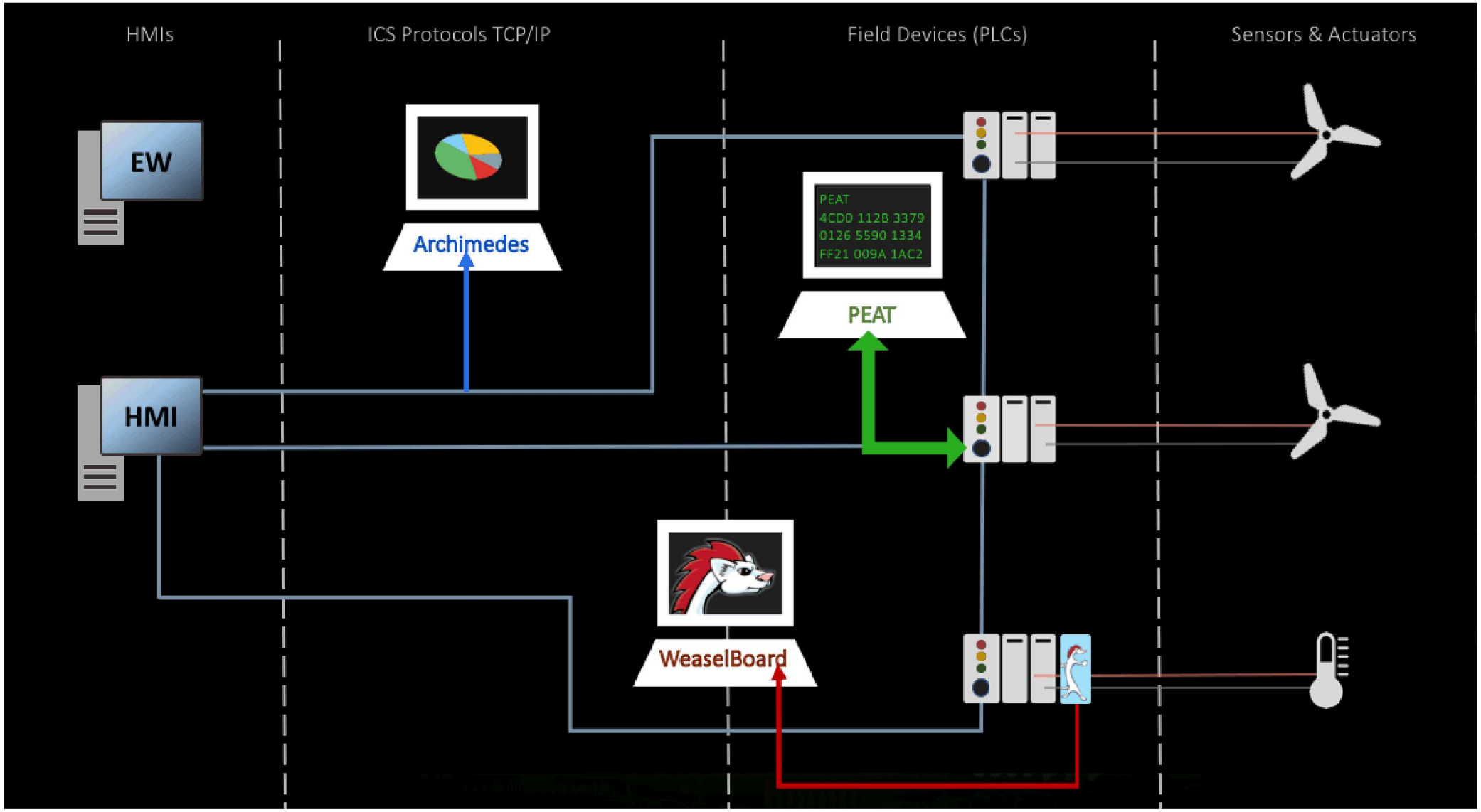
Field Device Internal Communications: Weaselboard Detection

When a rule is violated, WeaselBoard sends a Syslog alert
- In-band over SSH
- Out-of-band from WeaselBoard's (isolated) Ethernet port

Rule examples
- Alert when process logic update attempt crosses the backplane
- Alert when firmware update attempt crosses the backplane
- Alert when the process defies the laws of physics
  - Rotation was 5000 rpms. One second later it's -5000 rpms

WeaselBoard can also stream backplane traffic over the Ethernet port
- Instead of alerting

Multiple Layers of ICS Network Scanning



What Is Improved By Our Research? Process Knowledge

Asset identification

- “As is”, not “as designed”
- More detailed than vendor ID from MAC address
- Site-specific device information

Real-time Situational Awareness

- Visualization of regular process behavior
- Independent verification of HMI
- Verification of signal path, no MITM: HMI -> OPC -> PLC -> actuators

What Is Improved By Our Research? Anomaly Detection

Real-time

- Detect new software behaviors (as in Crash Override)
- Observe firmware update over network and backplane

Zero-Days

- Observe behavior instantly
- Detect the heist, not the break-in

Next Steps

Automatic comparison of different layers' results

Alerts at multiple layers (network, process, device)

Have tools for detection, need tools for reaction

Limitations

Each of these tools is designed/written for a specific protocol or device

- Time consuming
- Expensive

Lab testing is only so realistic

Machine-learning on lab-generated data is limited (we are always looking for real data)

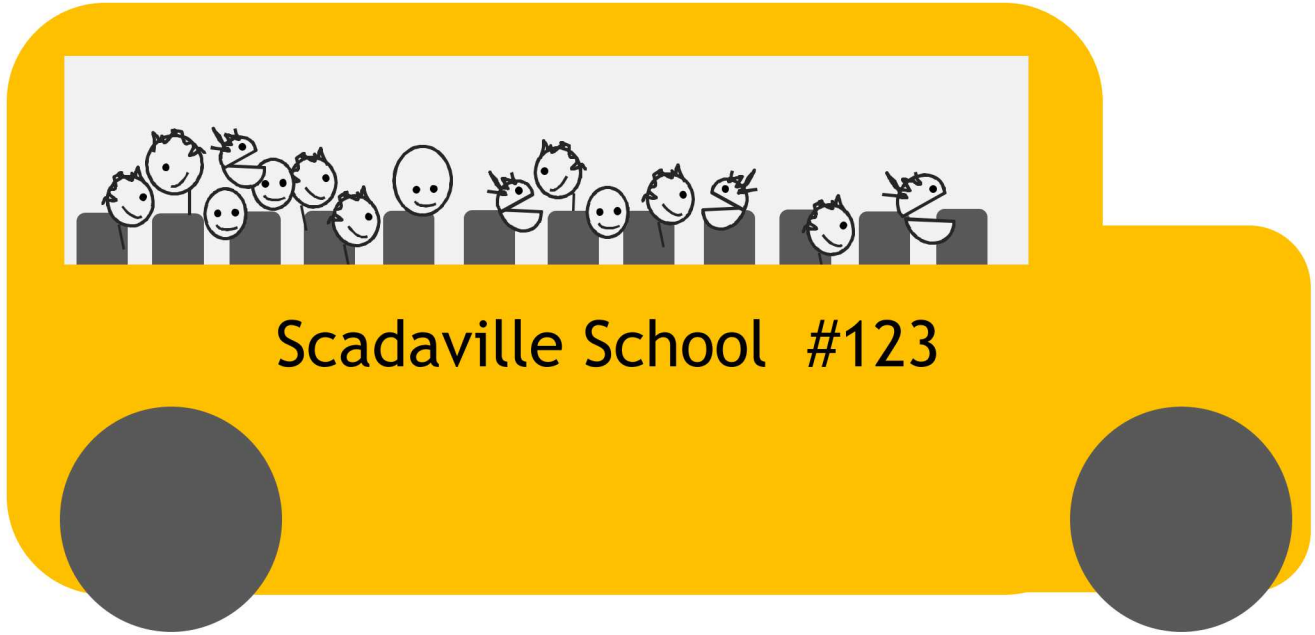
Encryption stops validation!

- Tools require unencrypted ICS traffic

Authentication Over Encryption

Unencrypted, authenticated control traffic is like a school bus

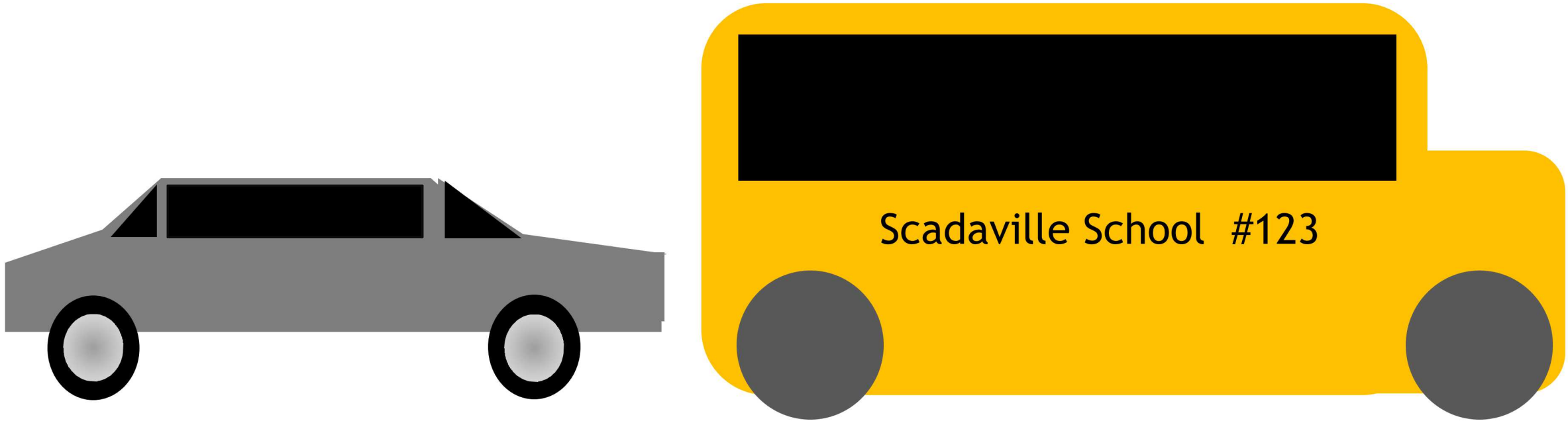
- only goes certain places
- only moves certain things
- none of this is a secret



Authentication Over Encryption

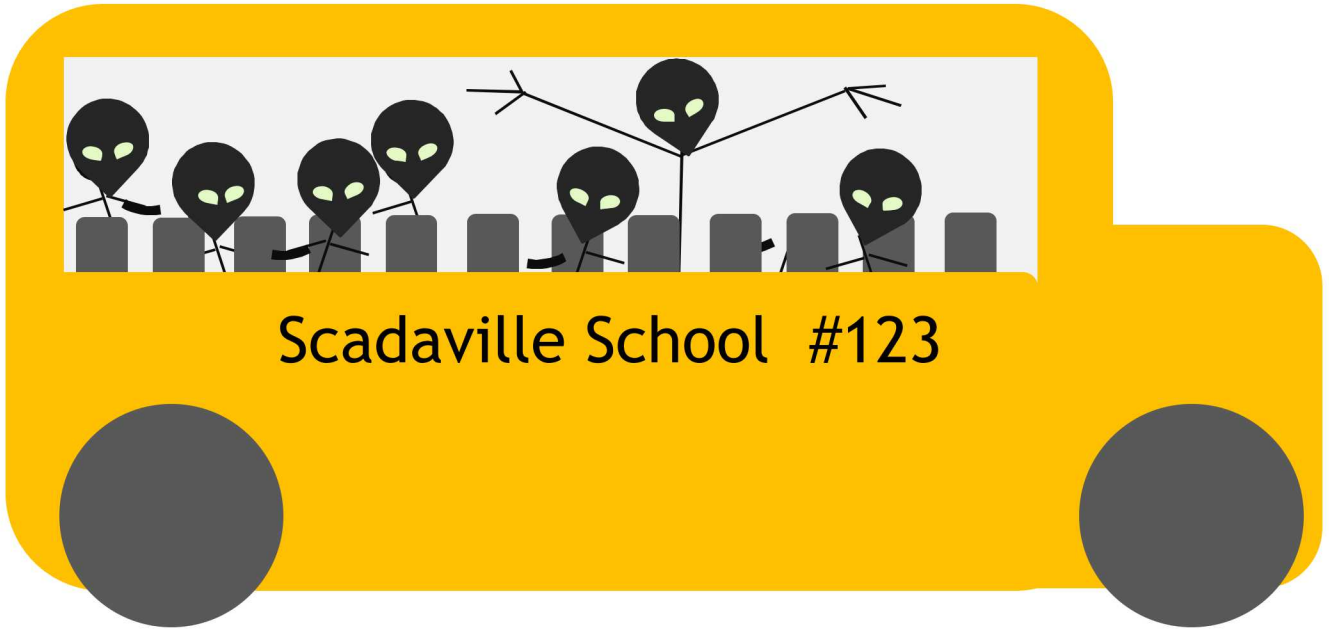
Encrypted IT traffic is like a limousine with blacked-out windows

- it goes anywhere
- it moves anything
- the contents are a secret



Authentication Over Encryption

If process values are wrong, we want to know ASAP!



Authentication Over Encryption