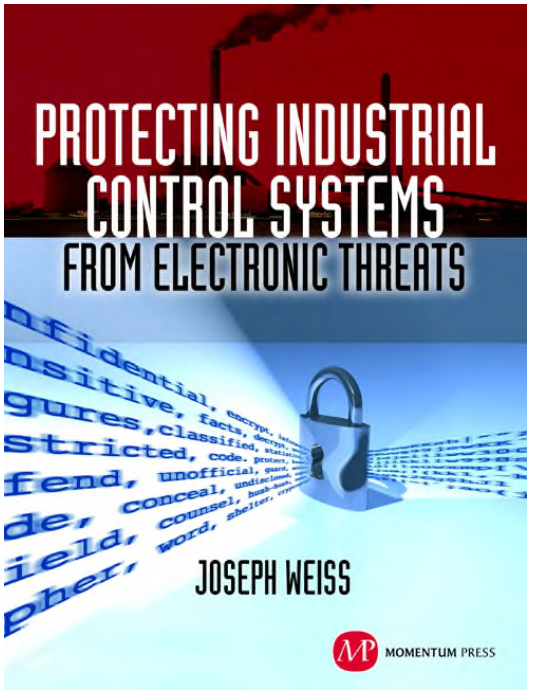
Changing the Paradigm of Control System Cyber Security

September 27, 2018



Joe Weiss
PE, CISM, CRISC, ISA Fellow
Managing Partner
Applied Control Solutions, LLC
joe.weiss@realtimeacs.com

Definitions

- Cyber incident
  - Electronic communication between systems that affects either Confidentiality, Integrity, or Availability
  - EMI/RFI can be considered cyber if they affect control systems
  - Doesn't have to be malicious
  - Doesn't address safety
- Edge device
  - Control system devices such sensors, actuators, drives
  - Not IT devices such as cell phones, laptops, routers
- Risk – F*C, don't know either term
- …

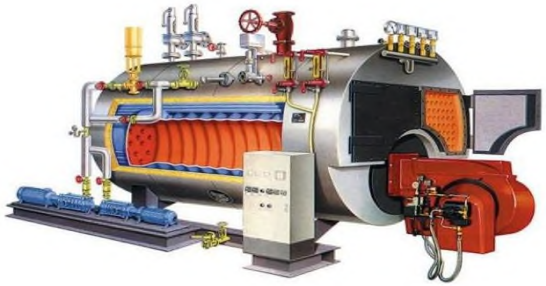
Changing the Paradigm

- Current IT approach is monitor the network for vulnerabilities/malware
- Engineering focus is reliability, availability, productivity, and safety
  - Process sensors, actuators, and drives directly affect all 4, have no security, and can be hacked with minimal forensics
- Adequately maintaining these requirements maintains security; however, the converse may not be true
- If cyber can't impact the 4 key requirements, cyber is not important for control system cyber security!

Change in Focus is Needed

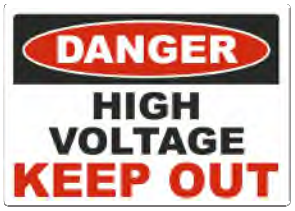
- Current approach is IT-focused and is untractable

- Need to make it an engineering problem which can be solved



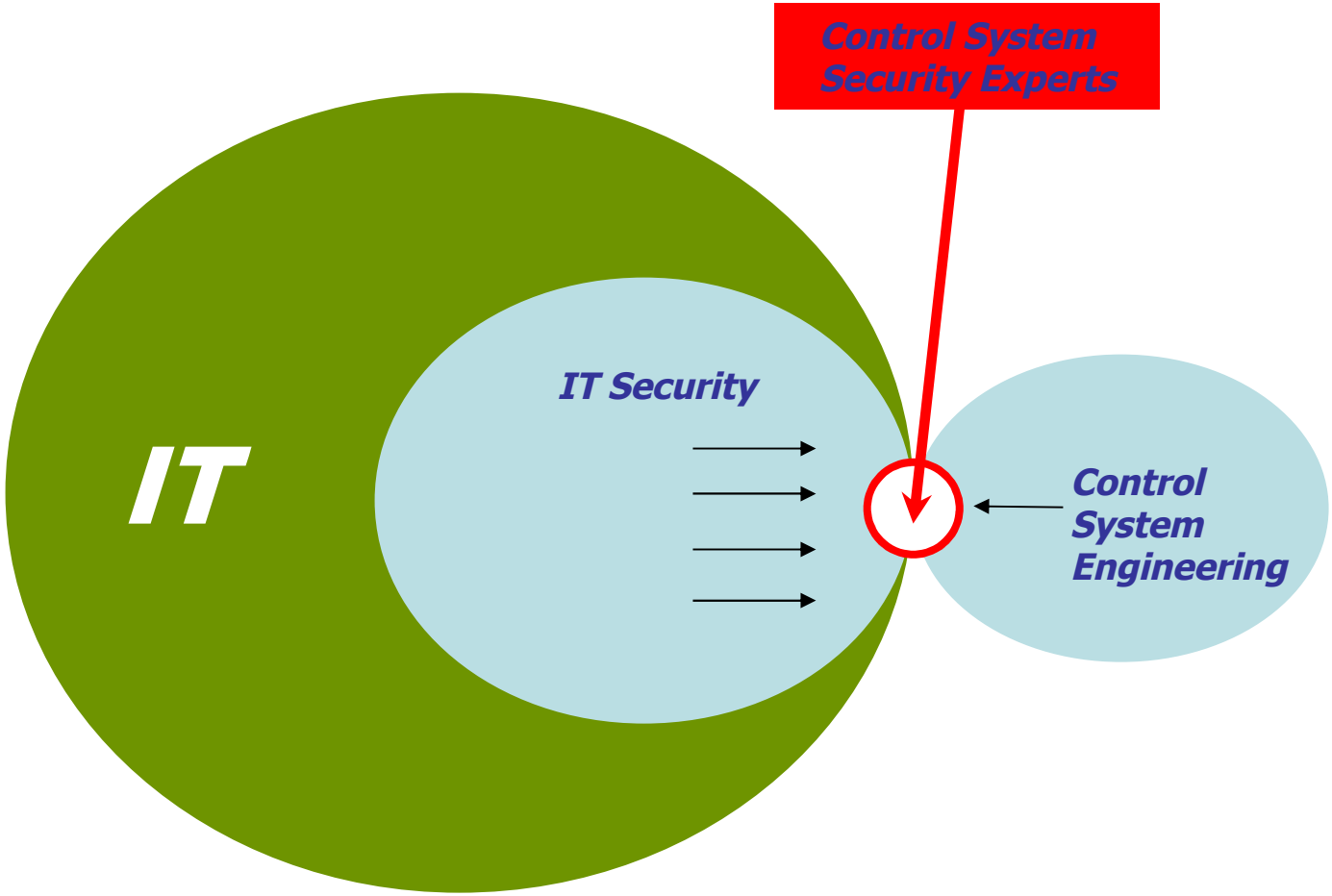
Physical Processes can be Dangerous

What we worry about

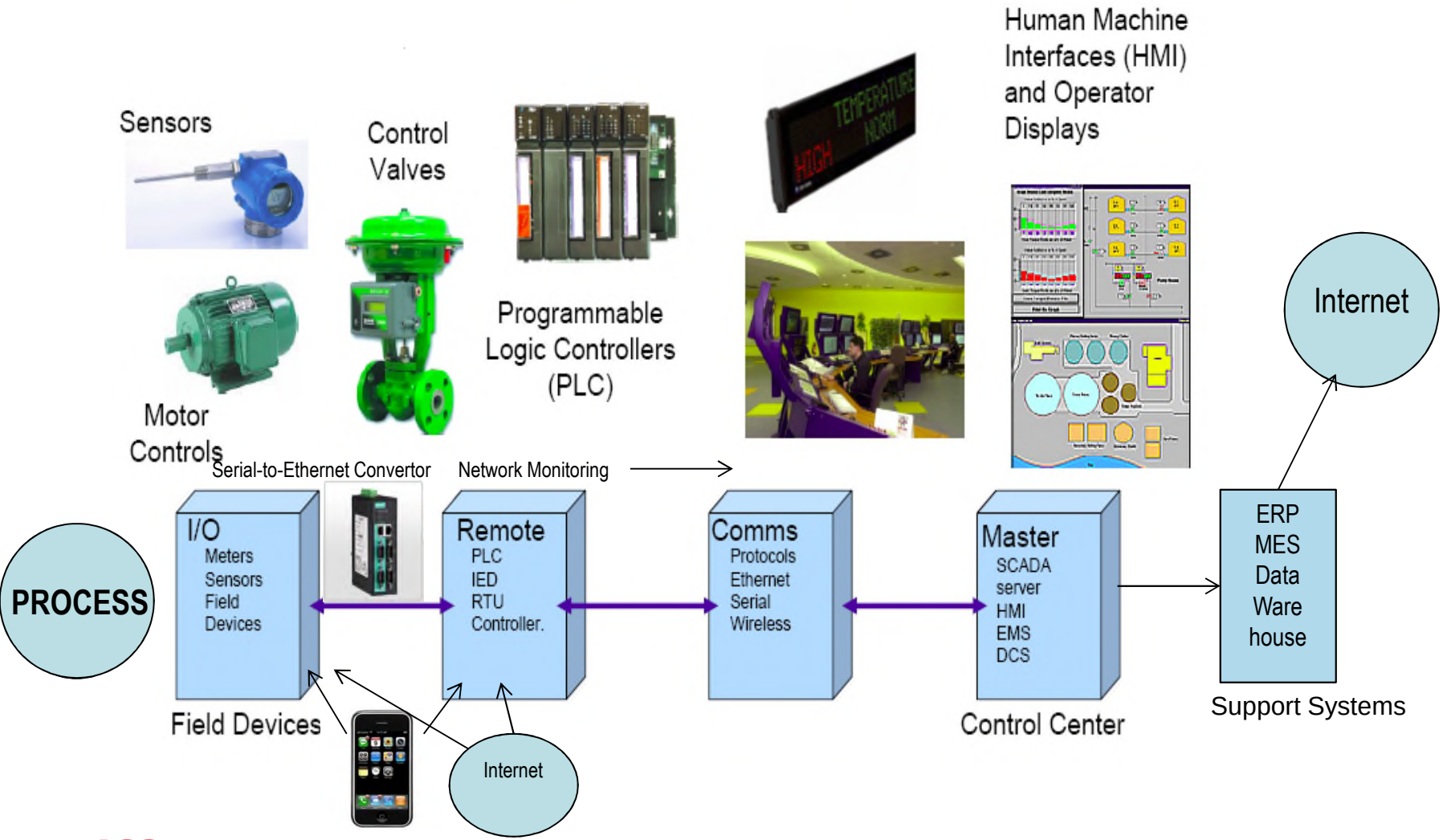


What we don't worry about

Control System Security Expertise Lacking



Control Systems Basics



Comparison of IT and Control Systems

Attribute	IT	Control Systems
Confidentiality (Privacy)	Very High	Low
Message Integrity	Low-Medium	Very High
System Availability	Low-Medium	Very High
Authentication	Medium-High	High
Non-Repudiation	High	Low-Medium
Safety	Low	Very High
Determinism (Timing)	Low	Very High
System Downtime	Tolerated	Not Acceptable
Security Skills/Awareness	Usually Good	Usually Poor
Network Monitoring	Most Important	Important
Patching	Expeditious, Generic Patch	Deferred, ICS Vendor Patch
Field Devices (Process Sensors)	Not Important	Very Important
System Knowledge	Usually Poor	Very Good
System Lifecycle	3-5 Years	15-25 Years
Interoperability	Not Critical	Critical
Computing Resources	“Unlimited”	Very Limited
Applicable Standards	ISO27000	ISA/IEC62443

Examples of Recent ICS Cyber Events

- Numerous cyber attacks affecting operations/hardware
  - Chip plant shutdown
  - Power lost to 20,000+ customers in US
  - British Airways data center compromise
  - Honeywell thermostat server issues
- Russian attacks
  - DHS disclosures about “Russia in control rooms”
  - NERC Lessons Learned - Russian ransomware affecting grid equipment
- Iran aware of Level 0,1 lack of security

UPS Cyber Issues

- >200,000 power devices on the web including a combined 100,000 UPS's, PDU's and Battery monitoring systems.
- NO passwords required to get into the unit or to get to the system configuration screen
- Card manufactured by Megatech used by a number of US UPS manufacturers.
- Hundreds of thousands of these types of cards in service
- Options:
  - Drain the battery in a full battery test until its low,
  - Cause the UPS to shut down in a power failure or glitch,
  - Put the UPS into sleep mode indefinitely, etc.

From Bob Hunter

Control System Cyber Incidents Are Real

- >1,000 incidents to date
- Impacts ranged from significant discharges to significant equipment damage to major electric outages to deaths
  - >1,000 deaths to date
  - >$60 Billion in direct impacts
- Very few ICS-specific cyber security technologies, training, and policies
- >2 million ICS devices directly connected to the Internet (and counting)
  - Many are gateways
- Resilience and recovery need to be addressed









What Are ICS-Unique Cyber Threats?

- Cyber-physical, not just the network
- Limited number of vendors supporting end-users world-wide
- Persistent Design Vulnerabilities, Not just Advanced Persistent Threats
- Want undetected control of the process, not denial-of-service

Gap in protection of the process (Purdue Reference Model Level 0)

- eg, Aurora, EMI/RFI

Compromise of the measurement ((Purdue Reference Model Level 1)

- eg, HART vulnerability

Compromise design features of the controller (Purdue Reference Model Level 2)

- eg, Stuxnet

EMI in Industrial Control Systems

November 1999, the U.S. Navy was conducting exercises off San Diego during which, two commercial spectrum users experienced severe electromagnetic interference (EMI) to their Supervisory Control and Data Acquisition (SCADA) wireless networks operating at approximately 928.5 MHZ.

The San Diego County Water Authority (SDCWA) and the San Diego Gas and Electric (SDGE) Companies were unable to remotely actuate critical valve openings and closings as a result. This necessitated sending technicians to remote locations to manually open and close water and gas valves.

The cause of the EM interference was determined to be a Navy AN/SPS-49 radar operating off the coast of San Diego.

SCADA EMI Resulting In A Natural Gas Pipeline Failure

- Natural gas pipeline SCADA system located 1 mile from the Naval port of Den Helder, Netherlands
- EMI was traced to an L-band Naval radar coupling into SCADA
- SCADA disturbance caused a catastrophic failure of roughly 36-inch diameter pipeline, causing a large gas explosion
  - RF energy caused the SCADA system to open and close a relay at the radar scan frequency (6-12 rpm), which was in turn, controlling the position of a large gas flow-control valve
  - Resulting changes in valve position created shock waves that traveled down the pipeline causing pipeline failure

Aurora Vulnerability Demonstration

Level 0 –The Process

Aurora Vulnerability – What is it?

Aurora Vulnerability

Programmable Digital Relay

- The Elements Necessary for an Attack
  - Programmable Digital Relay
    - Or other device that controls the breaker
  - High-Speed Breakers
  - Access (front panel, modem, Internet, wireless, or SCADA)
  - Laptop/Desktop Computer
- Knowledge Necessary:
  - Power Engineering (attack planning and device setting skills)
  - Hacking Skills (exploit the relay and conduct the attack)
- Time Required to Conduct the Attack (after gaining access):
  - Less than one minute
  - No additional software is introduced
  - Uses the internal settings of the imbedded relay software

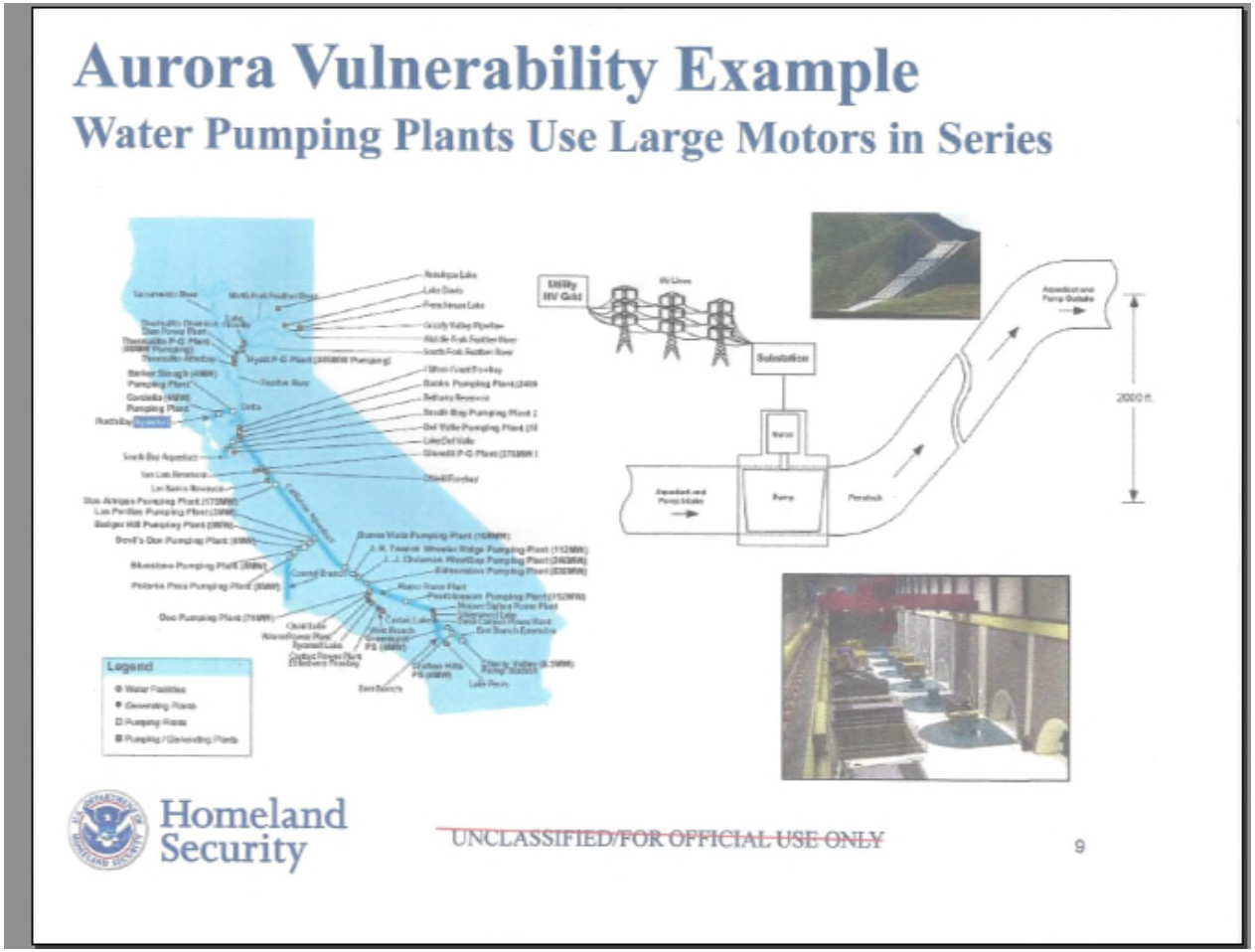
Homeland Security

~~UNCLASSIFIED/FOR OFFICIAL USE ONLY~~

8

Aurora Vulnerability Impacts

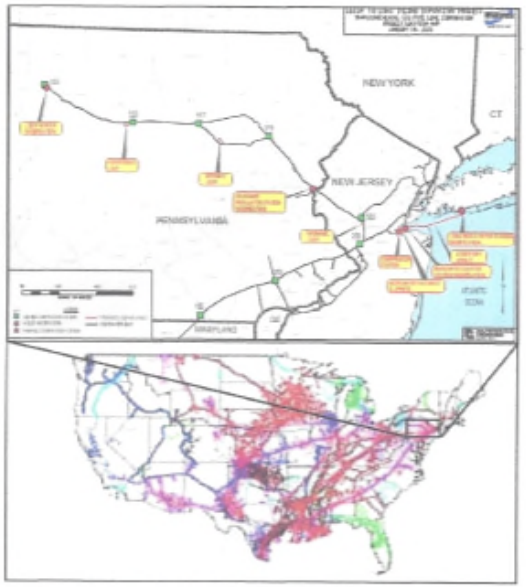
Aurora Vulnerability - Impacts



Aurora Vulnerability - Impacts

Aurora Vulnerability Example

Gas Line Compressor Stations Use Large AC Induction Motors Near Cities



Homeland Security

UNCLASSIFIED/FOR OFFICIAL USE ONLY

10

ICS Cyber Security Culture Issues

- Level 1 viewed as engineering systems – no security
- IT views cyber security as the network – not looking at the sensor and field devices before becoming packets
  - Can be analog or digital
- IOT/IIOT generally ignoring “edge ICS” (Level 1) devices
  - Affects all industrial clouds
- Vulnerability assessments assume there is some level of security
  - Gap analysis – infinite for Level 1
- ICS CERT 2016 ICS Cyber Incidents
  - 290 ICS Incidents
    - Spear phishing (26%),
    - Network scanning and probing (12%)
  - **No mention of Level 1 issues**

Olympic Pipeline Rupture

- Broadcast storm shutdown SCADA and Delayed Leak Detection
  - Loss of View, Loss of Control
- All sensors set to average values and safety systems didn't actuate
  - Loss of Safety
- Requires revisiting cyber security and safety standards

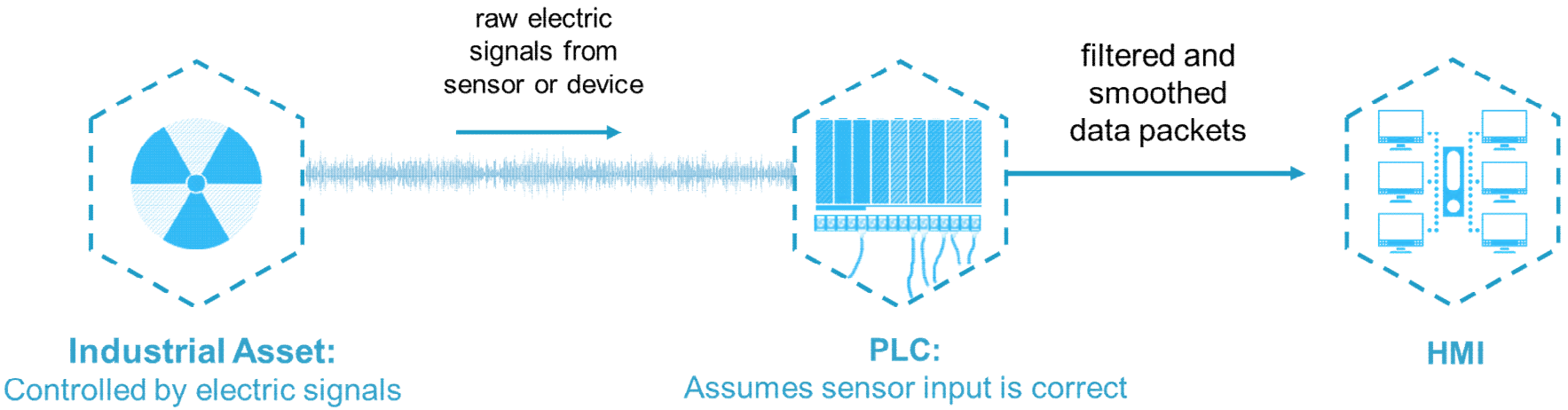
Benefits of Monitoring Sensors

- Real time sensor data can be used to:
  - Provide granular situational awareness
  - Help with cyber or equipment failure response
  - Help to find supply chain issues
  - Extend maintenance/testing intervals
  - Improve first principles models
  - Help refine operator response
  - Optimize equipment performance such heat exchanger effectiveness
  - Improve existing predictive maintenance programs
- Bottom line: ROI for cyber as most incidents won't be cyber

What is Being Done

- Demonstrations of hacking process sensors – it's real
- Proof-of-concept testing of sensor monitoring technology and its benefits
  - Power plant (use case 1), Chemical plant (use case 2), water plant (use case 3), water level control (use case 4)
  - Building controls
  - Additional test cases
- ISA99 established new Task Group to address Level 1 devices – ISA99WG4TG7
  - Scope is to identify IEC62443 standards that address, or should address, Level 1 devices for adequacy
  - Also looking at the definition of "Level 0,1" , "sensors", etc.

Is Process Sensor Data Trustworthy?

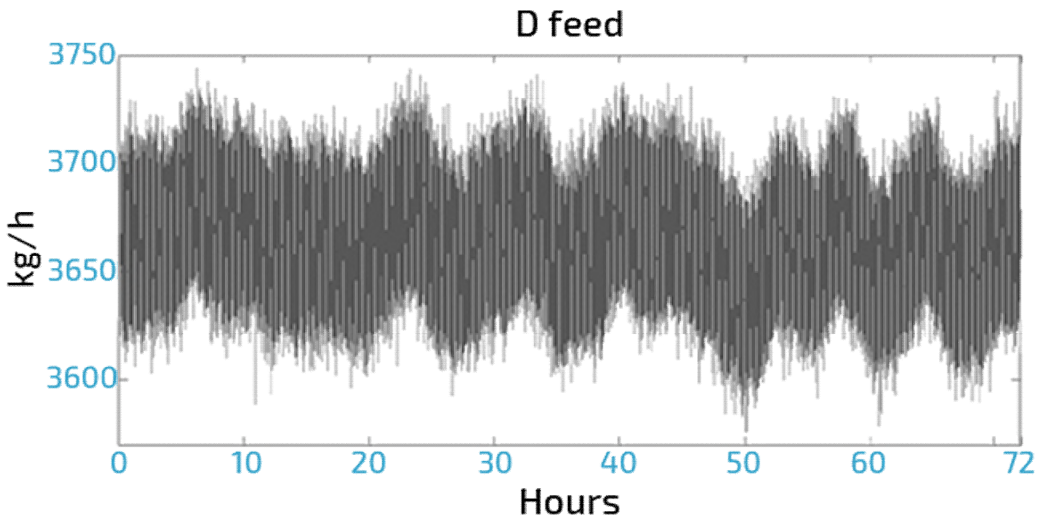


Operators often do not have a reliable picture of the health of the asset or process

Sensors drift or have other deviations

Equipment and sensor anomalies are found at the “physics” not packet level

Raw Signal Measurement Challenges



Raw sensor data rarely can be used directly

- Electrical output of sensing element has higher frequency components
- Raw signals subjected to signal conditioning such as amplification, filtering
- Higher frequency components indicative of offset, sensitivity errors, nonlinearities filtered out

CLIENT CASE STUDY #1

Accurate identification of fault avoids turbine downtime- Predictive Maintenance

Client:	Electricity Generation: Israel Electric Corporation (IEC)

Challenge:

A GE Mark V gas turbine failed to stabilize and deactivated upon fuel feed. Even after replacing a control card on the main controller, the situation still could not be remedied. Costly turbine outage was scheduled.

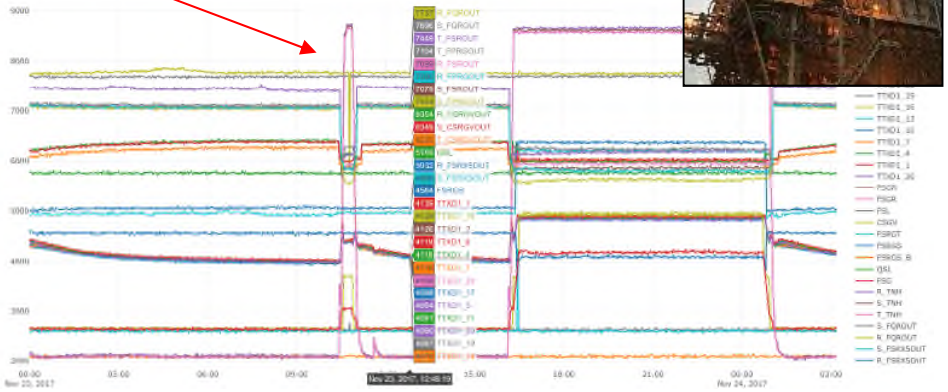
Solution:

The new technology showed an activation cross-fire (bad temperature sensor) that was not visible from HMI. The resulting adjustment allowed for safe turbine activation without costly outage.

Results:

The technology's ability to precisely identify the exact location and character of the fault by cross-correlating sensor readings enabled an immediate resolution, avoiding costly downtime

ISRAEL ELECTRIC CORPORATION



CLIENT CASE STUDY #2

Identification of production anomaly – Asset Optimization

Client:	Petrochemical Process: Israel Chemicals Ltd. (ICL)

Challenge:

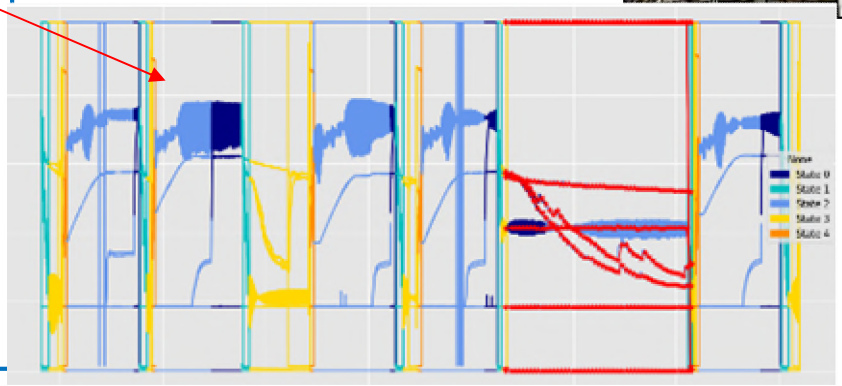
Bromine reactor anomalies in pH values have a direct impact on production quality and volumes

Solution:

The technology quickly identified a previously undetected anomaly at the source, showing that a critical process exceeded the norm, changing pH values and decreasing production parameters

Results:

Early identification of the pH process failure enabled immediate correction, saving raw materials and vital process time and allowed for clarification of work procedures and reporting



CLIENT CASE STUDY #3

Early detection of pending fault - Improved cyber security and resilience

Client:	Water Treatment: Jerusalem Water Authority

Challenge:

Existing predictive maintenance was not adequate to address reservoir pump status and process health.

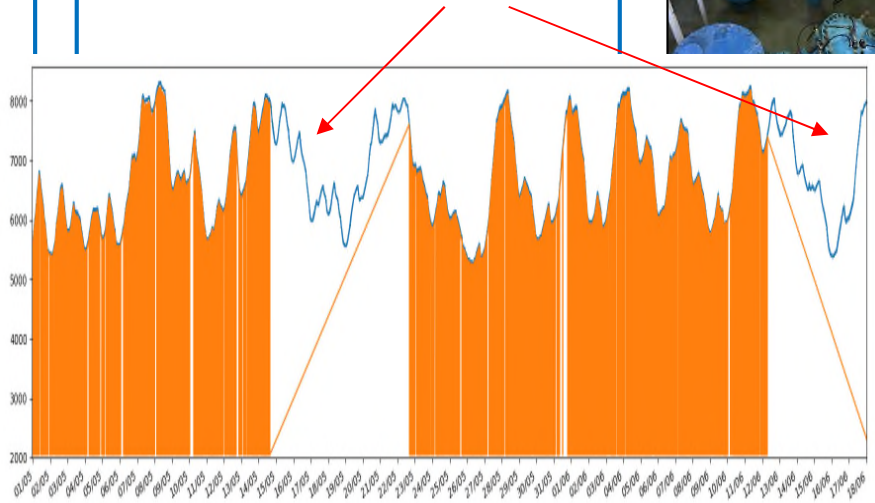
Solution:

The technology monitors more granular data **(in blue)** than SCADA **(in orange)**. Also, the technology is independent of the SCADA HMI, providing an additional measure of control and resilience.

Results:

The technology identified an impending pump fault and provided additional system resilience.

HAGIHON



CLIENT CASE STUDY #4

Monitoring Canal Water Levels to Prevent Flooding – Asset management

Client:	Metropolitan Water Reclamation District of Greater Chicago

Challenge:

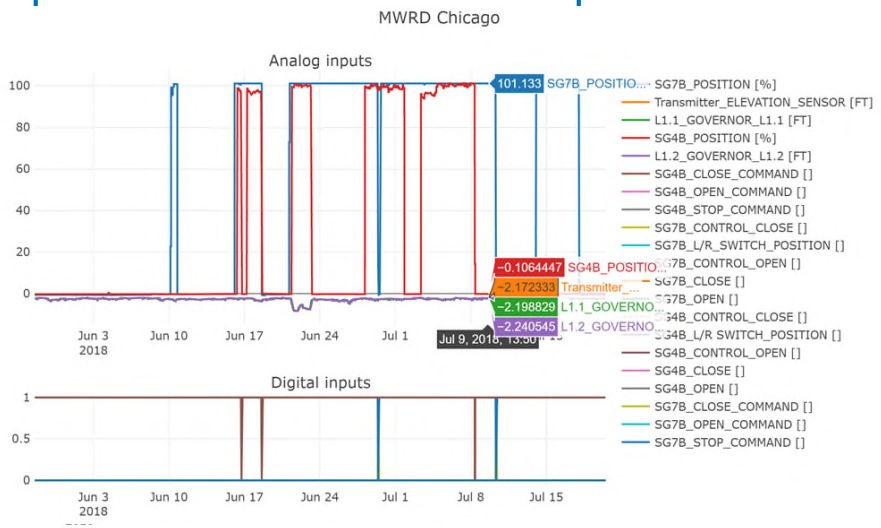
MWRD's main purpose is the reclamation and treatment of wastewater and flood water abatement in Chicago and Cook County to protect the health and safety of citizens and of area waterways.

Solution:

The technology has been installed at MWRD's Lockport Powerhouse on the Chicago Sanitary & Ship Canal, a facility that generates an average of 40 million kWh of electricity per year

Results:

Preliminary results illustrate the technology's ability to detect minute electrical signals not visible on MWRD's SCADA system



Key Outcomes from Case Studies

1. Validates process operations

- Autonomic system learns the process through data obtained directly from sensors, ***without knowing the process***
- Machine learning algorithm supports ***understanding of all processes***, correct readings of values, compatibility with the operating pattern
- Technology ***identifies any deviation*** related to changes in the dynamics of the process or sensor deviation
    - Includes cyber, supply chain, sensor drift, etc.

Key Outcomes from Case Studies

2. Detects process/sensor anomalies not identified by HMI

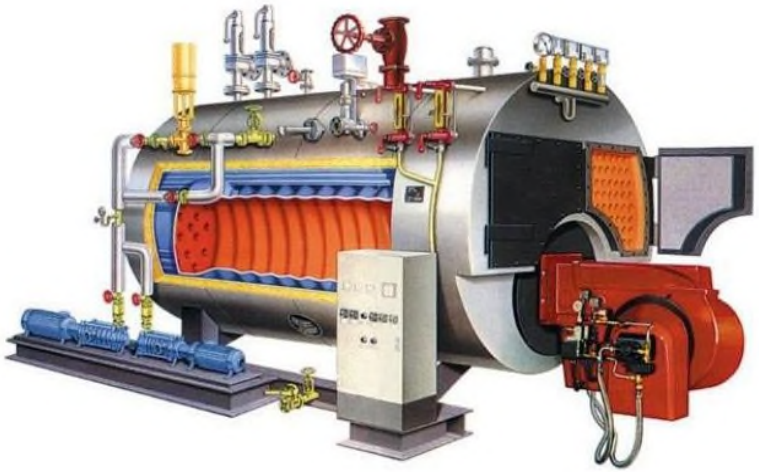
- Gateways are designed to filter and smooth “noisy” electrical signals to HMI
- However, process/sensor anomalies are identified through process noise/electrical signals
    - Sensor anomaly identified by granular monitoring

3. Continues to monitor operations independent of HMI

- Without HMI, technology continued to take readings and identify process anomalies providing improved cyber security and resiliency
    - Could have identified Stuxnet

The Cyber Holy Grail – Correlating Malware to Physical Impacts

Process anomaly detection ⟷ Network anomaly detection



Summary

- Cyber is real issue that can cause long term impacts
  - Doesn't require a nation-state
  - Minimal cyber forensics and technology for control system field devices
  - Change the paradigm to look at the process not just the network