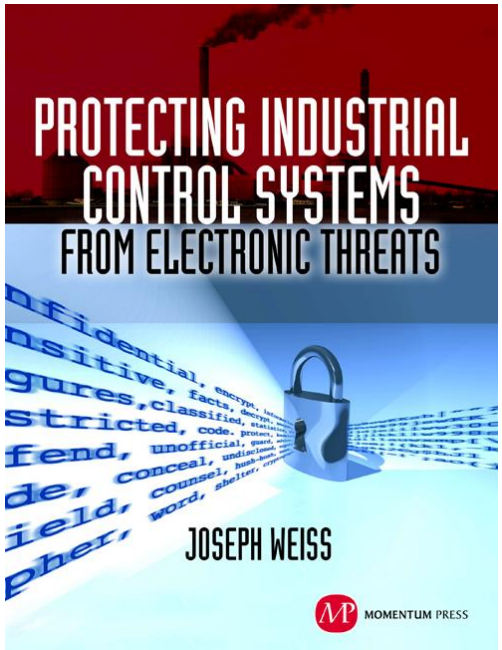
Control System Cyber Security – the Second Coming of the Maginot Line

Purdue Cerias Summer Series
July 15, 2020

Joe Weiss
PE, CISM, CRISC, ISA Fellow
Managing Partner
Applied Control Solutions, LLC
joe.weiss@realtimeacs.com
(408) 253-7934



Joe Weiss

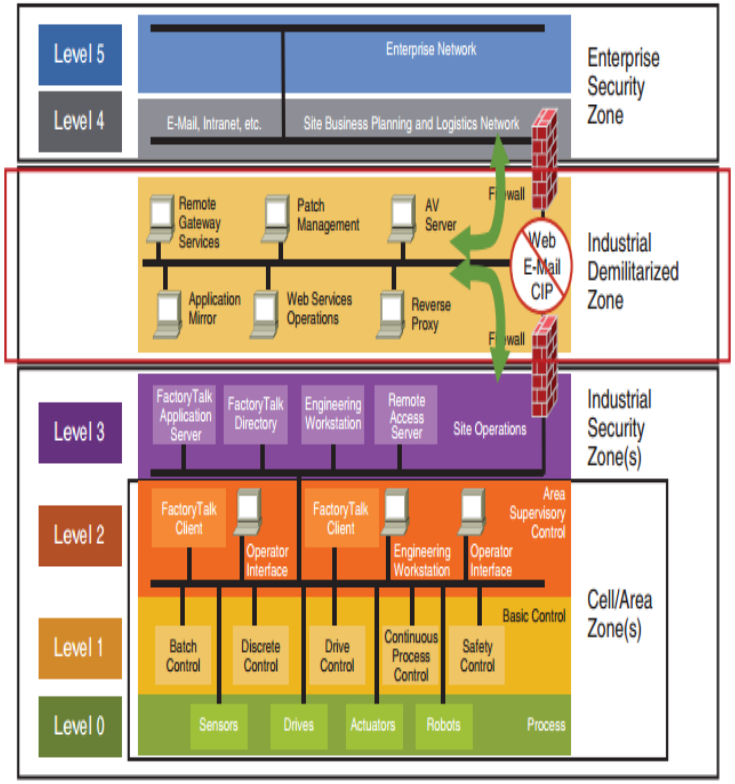
- I&C Engineer
- >45 years experience
- Started electric industry ICS cyber program in 2000
- Managing Director ISA99
- ISA Fellow, PE, CISM, CRISC
- Author- Protecting Industrial Control Systems from Electronic Threats
- Patents on instrumentation, control systems, and OT network monitoring

Control Systems are ubiquitous

- Control systems are critical to operating assets including power, refineries, pipelines, chemicals, manufacturing, water, military systems, medical systems, transportation, etc.
- Control systems include Distributed Control Systems – DCS, Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Intelligent Electronic Devices (IEDs), process sensors, actuators, drives, power supplies
- Control systems monitor and control physical processes in real time

Important definitions

- Cyber Incident
  - Defacto IT definition
    - Connected to the Internet, running Windows, and data is maliciously being manipulated or stolen - All about privacy
  - NIST definition
    - Electronic communication between systems that affects Confidentiality, Integrity, or Availability
    - No mention of “malicious“ or Safety
- Level 0,1 Devices
  - Not the OSI model



Confusing terms/definitions

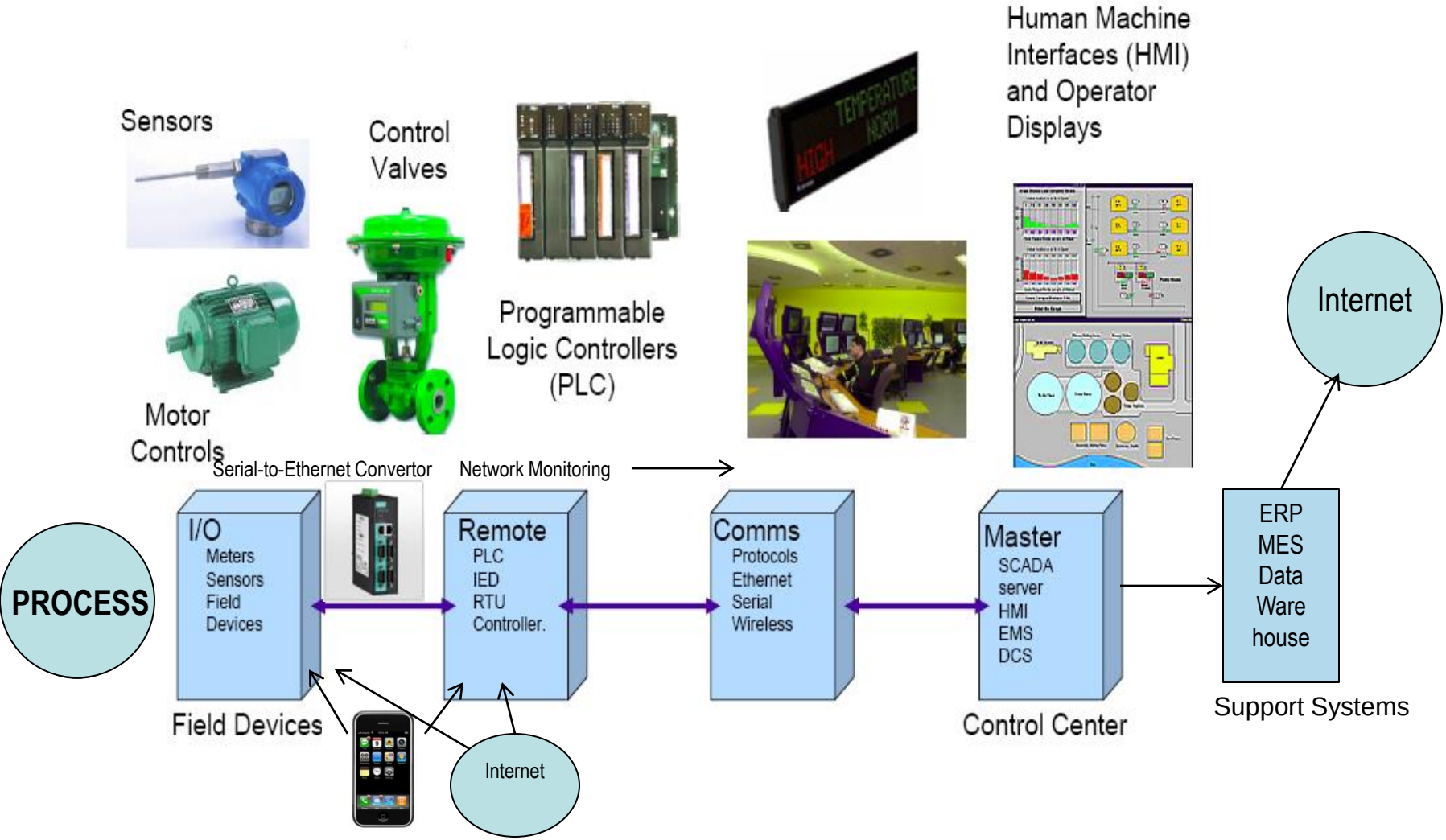
- "Smart" Cities, grid, sensors, manufacturing, water,…
  - Two-way communications and programmable – cyber vulnerable
- Digital transformation, Industry 4.0, IIOT,…
  - Starts with Analog
- Operational Technology (OT)
  - Control system networks, not control systems and plant equipment
- Physical-Cyber vs Cyber-Physical
  - Physical equipment with cyber connections
- Endpoints/Edge devices
  - Level 0,1 devices
- Malicious, Insider
  - VW cheat scandal

How did we get here?

- Prior to 9/11, cyber was just another risk for reliability and safety (Engineering involved)
  - Engineering owned everything including cyber
- Following 9/11, cyber became national security and moved to IT (Engineering often not involved)
  - Legacy engineering systems not part of the network - no security or authentication nor can they be upgraded
  - COTS systems are slow - sensor process noise indicative of sensor and process health removed

Cybersecurity “Maginot Wall” – only for IP networks

Control systems basics



Control system cyber incidents are real

- >1,250 incidents to date
- Impacts ranged from significant discharges to significant equipment damage to major electric outages to deaths
  - >1,500 deaths to date
  - >$70 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

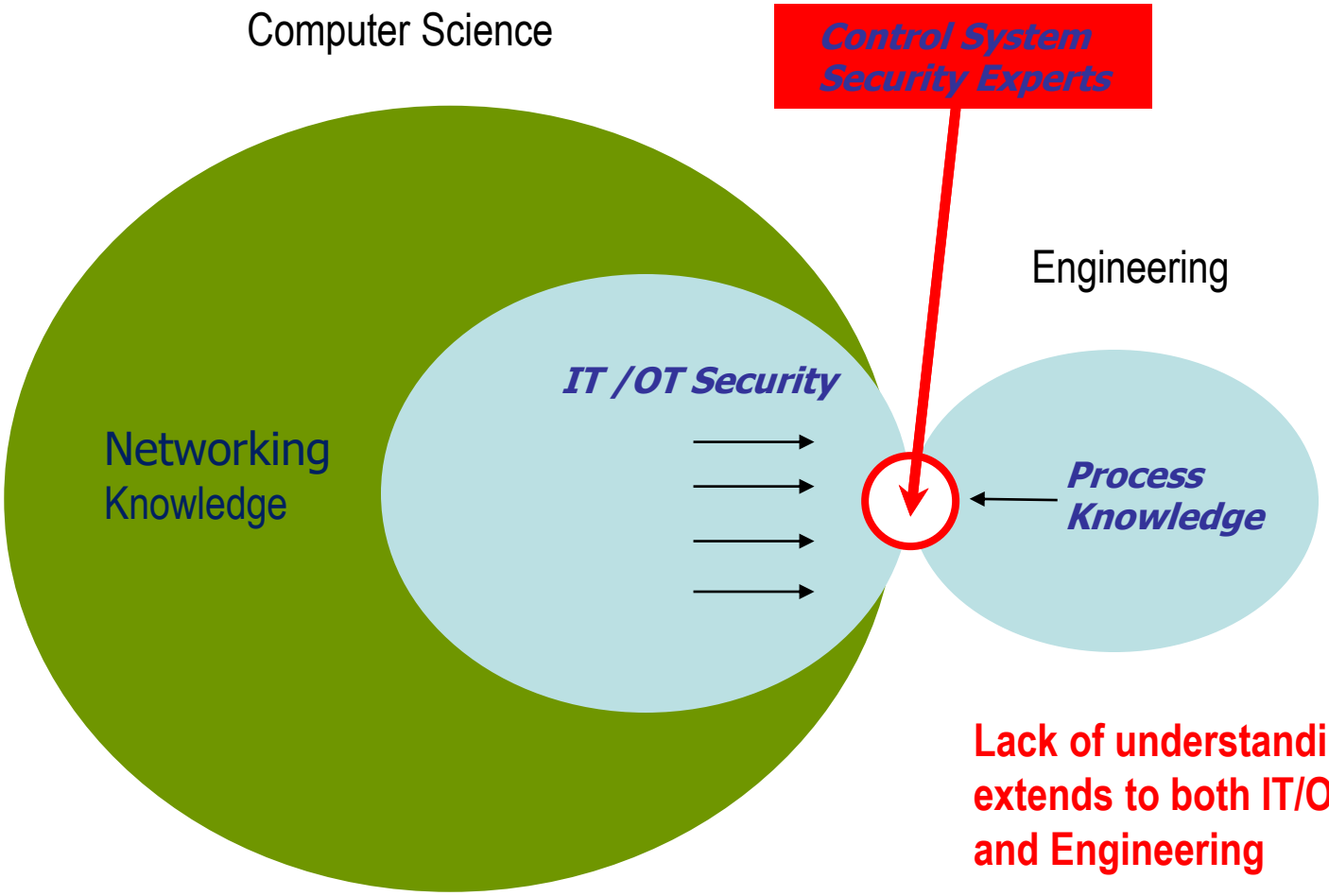








IT/OT vs Engineering - Packets vs Process



Misconceptions

- SCADA/HMI (master station) is used in all control systems
- SCADA/HMI is needed to keep lights on
- Operator can prevent damage
- Control system devices can only be accessed from Ethernet network
- All control system anomalies can be found from Ethernet network
  - (Necessary but not sufficient)
- Sensors/field devices are uncompromised, authenticated, correct
- Network vulnerabilities = physical system impacts
- Security = safety

Selected ICS Cyber Security Threats

- Most probable: Unintentional and network security experts
- Concerns for malicious attacks:
  - Knowledge of control systems and operations is universally known
    - Russia, Iran, China,… aware of ICS cyber security limitations
  - Limited number of suppliers so attacks can be wide-spread across multiple industries
  - Attacks can be made to look like equipment malfunctions
  - Limited ICS cyber forensics and training
  - Culture and governance issues

Attackers are becoming better systems engineers than the defenders

Culture/Governance gaps

- Frameworks are cyber-security focused
  - Don't address the need to keep the process functioning
  - Includes Solarium Commission report
- IT/OT and Engineering have different priorities
  - Engineering focused on process reliability and safety
    - Impacts important whether malicious or unintentional
  - IT/OT focused on networks
    - Focus is vulnerabilities and malicious data attacks
- Cyber decisions often made with no engineering participation
  - Unintended consequences from security technologies/testing

Physical-cyber attacks

- Stuxnet, Triton
  - Intent to destroy equipment without being detected as cyber attack
  - Attack on IP networks and Windows HMIs/workstation
  - Make the attack look like equipment malfunction
  - Replay displays, suppress alarms to confuse operators
- Impacts
  - Centrifuges being damaged for a year before malware found
  - June 2017 – plant trips – **no indications of malware in network or controllers** – plant restarts
  - August 2017 – plant trips – malware identified

Why Presidential Executive Order 13920

- Hardware backdoors and “field device knockoffs” found in large Chinese-made transformers
  - Can bypass cyber security and engineering safeguards
  - Can cause unexpected operation or confuse operators
  - Can cause equipment damage using vectors like Aurora or others
  - Can monitor power to know when we are most vulnerable
- Size of the problem unknown
  - >200 Chinese-made transformers in US energy sector
  - Other Chinese-made equipment, software, chips may be in domestic equipment
  - Chinese-made equipment used in multiple industries
- Potential scope and impact to the US grid unknown

Electric Industry Cyber Security has not Focused on Equipment in Executive Order

- The term “bulk-power system electric equipment” means items used in bulk-power system substations, control rooms, or power generating stations, including reactors, capacitors, substation transformers, current coupling capacitors, large generators, backup generators, ***substation voltage regulators (LTC),*** shunt capacitor equipment, automatic circuit reclosers, instrument transformers, coupling capacity voltage transformers, protective relaying, metering equipment, high voltage circuit breakers, generation turbines, industrial control systems, distributed control systems, and safety instrumented systems. Items not included in the preceding list and that have broader application of use beyond the bulk-power system are outside the scope of this order.

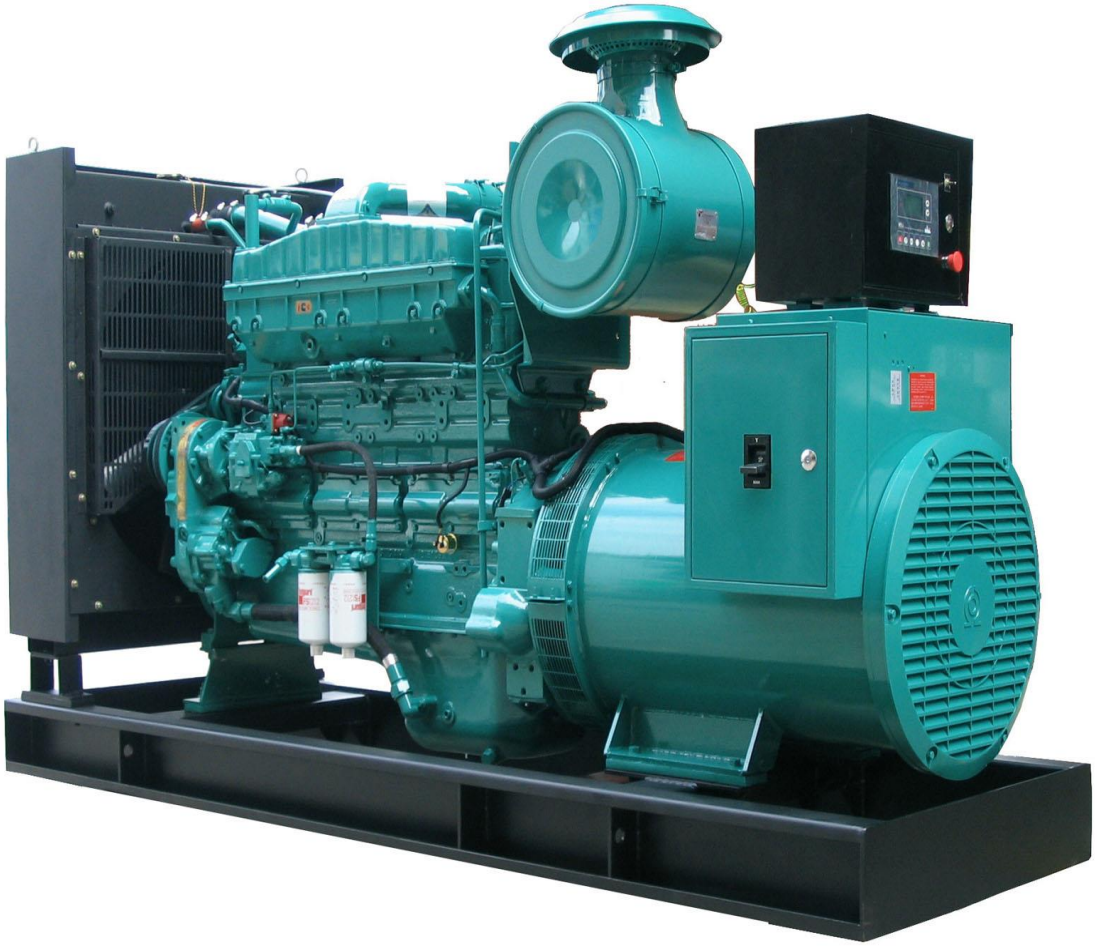
What Technically Needs to be Done

- Procurement requirements need to be reassessed
  - Develop cyber security requirements for equipment and field devices
- Supply chain needs to be validated
  - Know what's installed (counterfeits) and data validity (hardware backdoors)
    - Need process sensor technology for hardware (been demonstrated in lab)
    - Network penetration testing identified in DOE RFI doesn't address hardware
- Improved information sharing on counterfeits/compromised systems
  - Not just electric – Pharma facility compromised
- Address Governance issues between CISO and Engineering/Ops
- Factory and Site Acceptance Testing to include cyber considerations
  - Train field engineers
- Remote overseas connections should be reconsidered
- "Suspect" international field support to be reconsidered

What should be done if you can't stop cyber attacks – develop resilience

- Get over the culture gaps between security and engineering
- Isolate the control system devices to the extent possible
- Consider interlocks that can't be remotely changed
- Develop appropriate control system policies and procedures
- Develop appropriate system architecture
- Train the engineers to identify suspicious events
- Cross correlate equipment and network diagnostics

Equipment have sensor safety interlocks



If sensor setpoints set low, equipment cannot restart

If sensor setpoints set high, no safety

Sensors cannot be bypassed

Minimal forensics

Change the paradigm

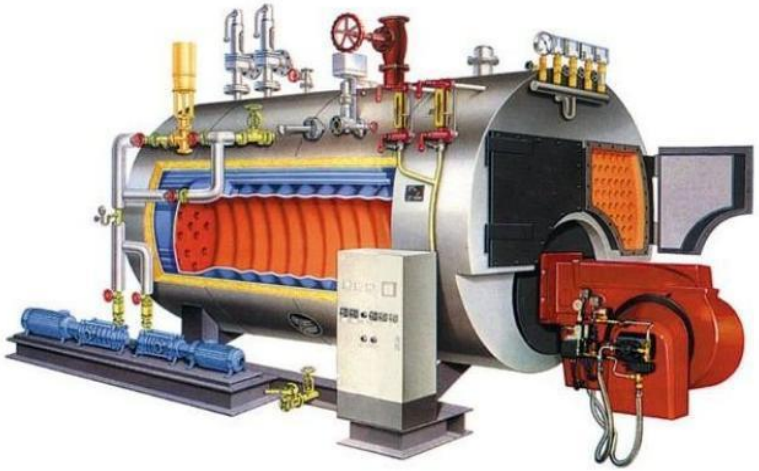
- Cyber security currently network anomaly detection
  - Can't correlate malware to specific equipment
  - Look from top down – what can the network do
- Make cyber security a by-product of process anomaly detection
  - Monitor sensors in real time – ground truth
  - If process unaffected, no cyber (or any other) issue
  - If process affected, cross correlate with network anomaly detection
  - If network affected, cross correlate with process as to whether to shut down
  - Looking from bottom up – what can happen to the process

Benefits from changing the paradigm

- Make an intractable network problem a tractable engineering approach
  - Requires collaboration between engineering and networking
  - Identifies deviations regardless of cause such as sensor drift, cyber, supply chain
- Create real ROI by validating/optimizing actual process operations
  - Process optimization, extend maintenance intervals, etc.
- Reduce cyber threat space and improve safety
  - View of the process independent of the cyber vulnerable HMI
  - Independent of Stuxnet, Triconix attack scenarios

The Holy Grail – correlating engineering physical impacts to network malware

Process anomaly detection (Engineering) ⟷ Network anomaly detection (Network security)



Recommendations

- Modify governance to include all affected organizations
  - Operations, maintenance, cyber and physical security, forensics, business continuity, procurement, communications,…
    - Have Engineering lead as they know possible unintended impacts
  - Develop control system cyber security policies based on actual incidents
  - Assure other policies do not impact control systems
  - Integrate operations and cyber alarm management/displays
- Make it an engineering issue
  - Assure that cyber issues cannot exceed design basis
  - Monitor sensors in real time
  - Train engineers to recognize possible cyber incidents
  - Incorporate into predictive controls and maintenance programs
- Cross train engineers, networking,… also affects universities

Joe Weiss
PE, CISM, CRISC, ISA Fellow
Managing Partner
Applied Control Solutions, LLC
joe.weiss@realtimeacs.com
(408) 253-7934