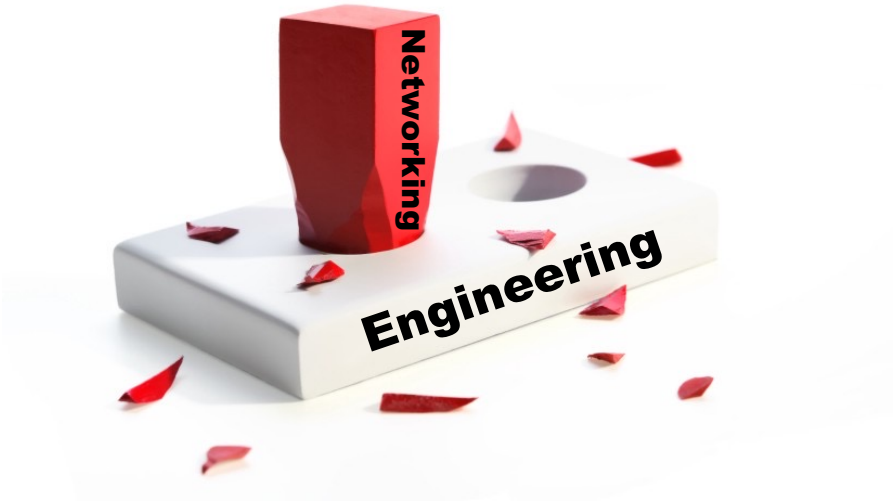
Control system cyber security-
The risks of putting a square peg in a round hole

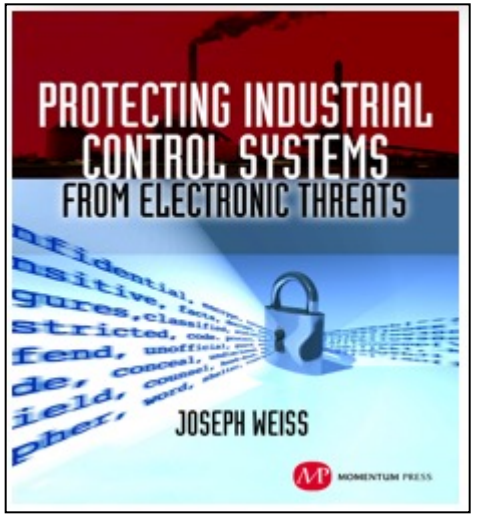
NPS Energy Academic Group
Defense Energy Seminar
November 1, 2022



ACS APPLIEDCONTROLSolutions

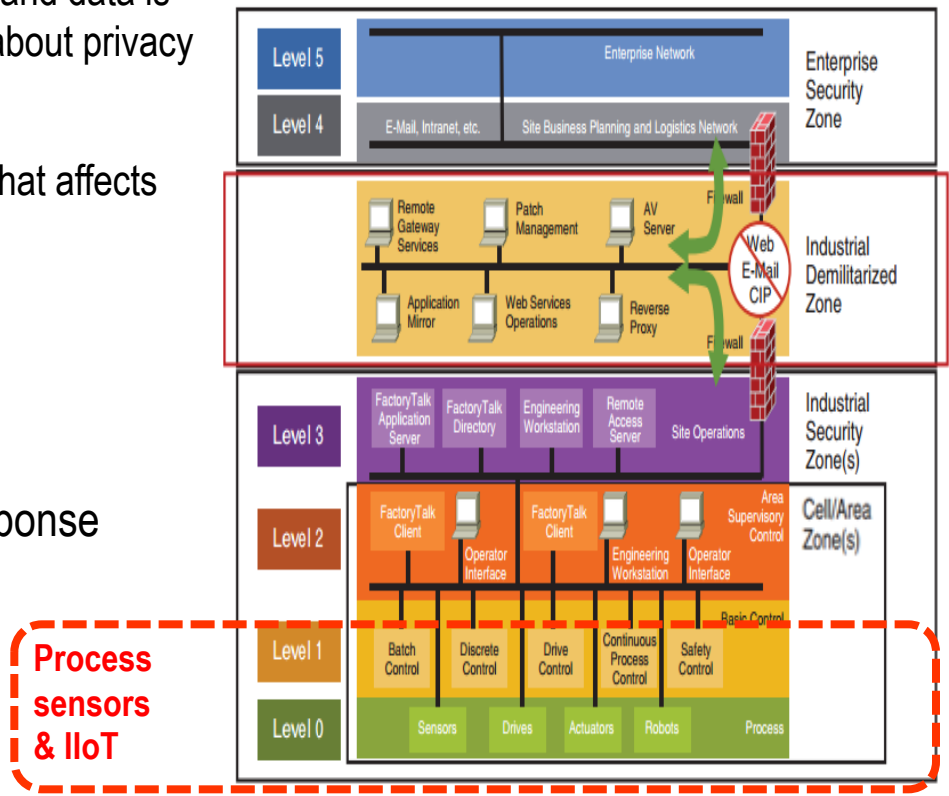
Joe Weiss

- I&C Engineer
- Over 45 years experience
- Helped start electric industry ICS cyber program in 2000
- Managing Director ISA99, ISA67, ISA77
- ISA POWID Achievement Award, ISA Life Fellow, PE, CISM, CRISC
- IEEE Senior Member
- Author- Protecting Industrial Control Systems from Electronic Threats
- Book chapters for electric, water, and data centers
- Patents on instrumentation, control systems, and OT network monitoring



Important definitions

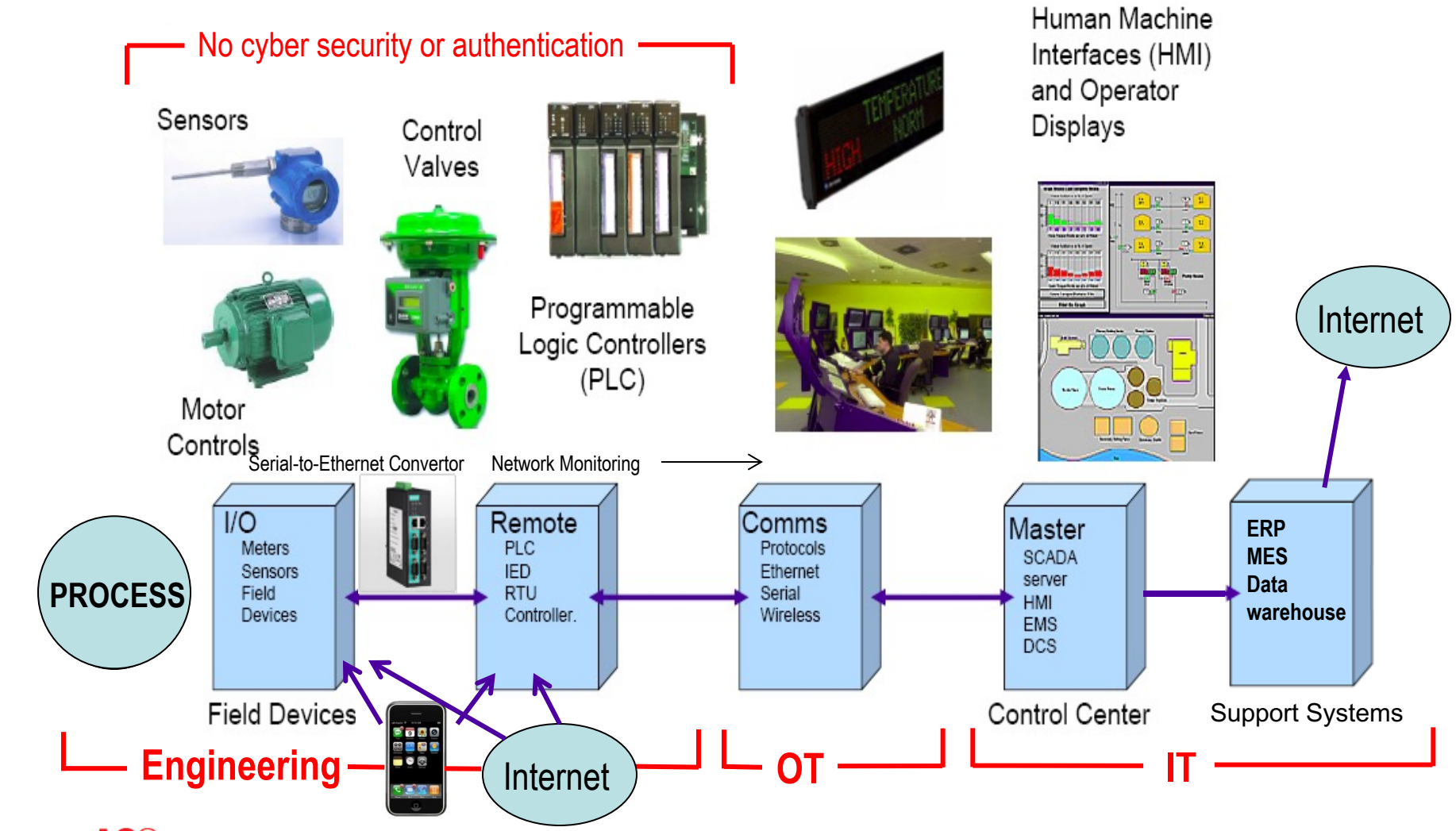
- **Cyber Incident**
  - Defacto IT definition
    - Connected to the Internet, running Windows, and data is maliciously being manipulated or stolen - All about privacy
  - NIST/GAO definition
    - Electronic communication between systems that affects Confidentiality, Integrity, or Availability
    - **Unintentional and Malicious**
- **Operational Technology (OT)**
  - Networks, not equipment
  - Focus is network visibility, detection, and response
- **Anomaly Detection**
  - IT/OT – network anomalies
  - Engineering – process anomalies
- **Level 0,1 Devices**
  - Not the OSI Model



Control systems are universal

- Russia, China, and Iran use same vendors with same equipment, same training, and same default passwords as in US
- US buys equipment and chips from China
- Control system standards development and use, including cyber security, have participation from all over the world including Russia, China, and Iran
- Same engineering disciplines are taught world-wide

Control system basics



What are process sensors

- Process sensors are devices that detect analog changes in their environment by measuring reactions to physical properties. The sensors use electronics to convert the reactions into recognizable measurements like temperature, pressure, level, flow, chemical composition, etc.
- Examples:
  - Thermocouples are 2 dissimilar metals that produce a voltage as the two pieces of wire heat up where the voltage is converted to temperature
  - Diaphragm-based pressure sensors produce capacitance signals when pressure is applied where the capacitance is converted to pressure
  - Radar level sensors use the time from when the signal is reflected by the top of the fluid to the time it returns and is converted to tank level.

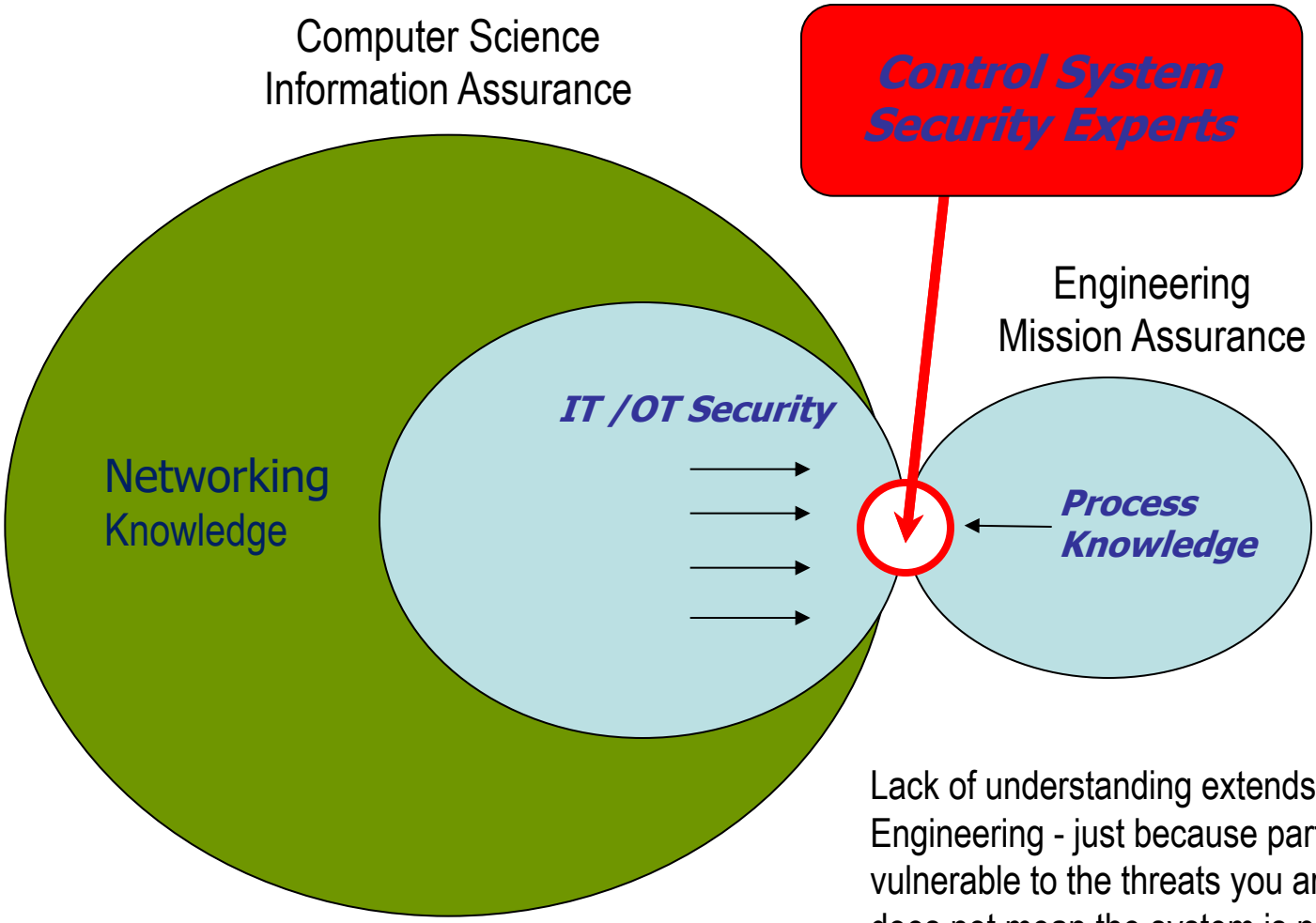
Process sensor issues

- Process sensors are used in every sector to measure pressure, level, flow, temperature, vibration, voltage, current, chemistry, etc.
- Process sensors are assumed to be benign and ignored by cyber security practitioners including the government and regulators – focus is network sensors
- Process sensors are the input to OT network monitoring programs
- ISA84.09 identified new process sensors failed 69 of the 138 cyber security requirements
- Process sensors cannot be upgraded for cyber security
- Abu Dhabi installed >3,000 new digital sensors that had no cyber security, passwords, or authentication

How large is the scope

- Renewables – 150 MW solar facility with 2 million panels with sensors and invertors on each panel
- Ship - 50-100,000 sensors
- Refinery/power plant - 20-40,000 sensors
- Large building - 10-30,000 sensors
- Electric Transformer – 10 sensors
- Water and sewer treatment facilities
- Pipelines, refineries, offshore oil platforms
- EV charging stations

IT/OT vs Engineering - Packets vs Process



Lack of understanding extends to both IT/OT and Engineering - just because part of the system is not vulnerable to the threats you are used to seeing does not mean the system is not vulnerable

Lack of engineering awareness (round hole)

- A key advantage of a mobile app solution over traditional handheld HART communicator is you can use the mobile device you already own. In addition to already owning the main piece of hardware required, it is typically upgraded every couple of years for a very low cost (if not for free). You are continuously getting more features and more processing power without any effort. Additionally, there are Bluetooth-based HART modems that provide great convenience.

- Fluke - The importance of calibration and maintenance software in electrical applications
  - No mention of cyber security

- Smart tools – Torque wrenches, pressure gauges, …
- Air Force Cyber College presentation: “Shields Up and Good Cyber Hygiene Don’t Apply to Legacy Process Sensors”
- Dale Peterson blog – 10/26/22 - Lack of authentication of process sensors is not a critical problem

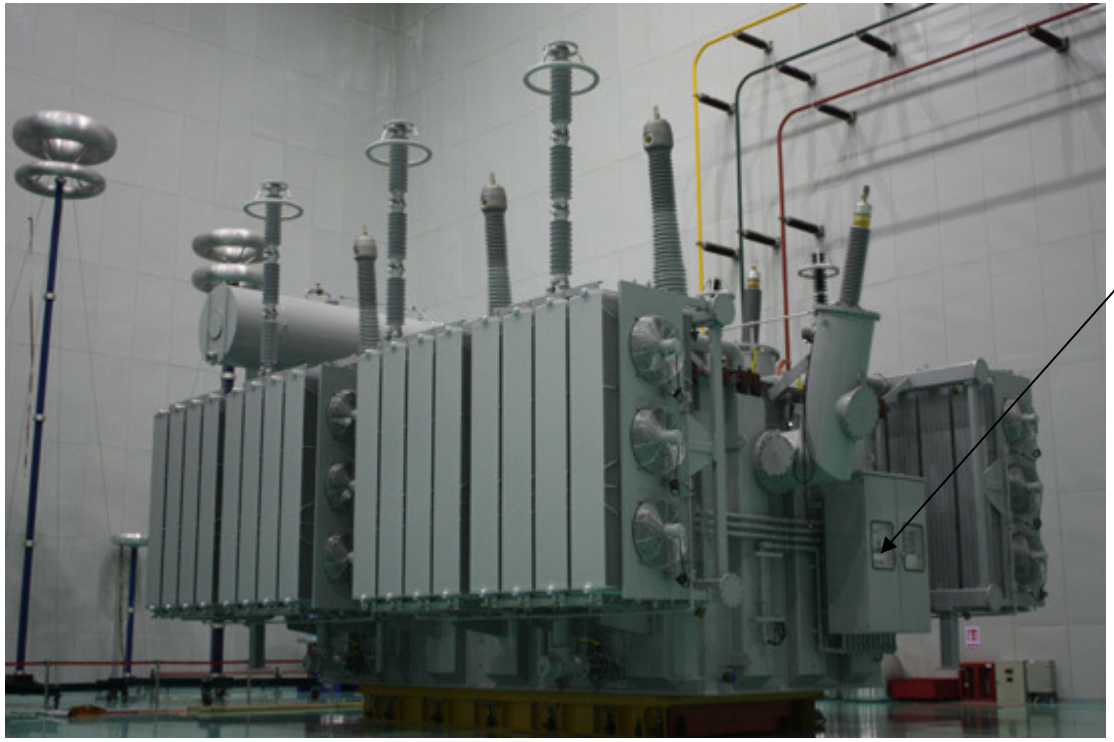
Lack of IT awareness (square peg)

- Digital loss prevention tools can harm ICS operation because many operational files are not static
- IT pen testing can harm control system devices
- IT patch management can harm control systems
- Anti-Virus can harm legacy control systems
- System hardening doesn't apply to field devices not running Windows
- Between January and September of 2021, a 2,204% increase, in adversarial reconnaissance activity targeting port 502 - Modbus
- …

Power transformer sensing

New transformer monitoring includes web visualization and remote parameterization. {This feature is generally used on key transformers deemed important by utilities but is not standard practice}

Cyber vulnerable protocols include IEC61850, DNP3, Modbus TCP, Modbus serial



Example: JSHP 345KV transformer (supplying 10% of the New York City load)

Sensors: Temperature, Voltage, Current, Power, Dissolved Gas, Oil Level, Gas Pressure, Bushing

Sensors provide input to: Alarms, Trips (Shutdowns), Start/Stop pumps, Stop/Start Fans, Circuit Breakers

What can go wrong if sensors compromised:

- Grid interruptions
- Mechanical or electrical failures
- Transformer fire or explosion,

Process cyber attacks

- Attackers use system weaknesses – defenders use network vulnerabilities
- Determine what to damage then determine cyber capabilities needed
- Exploit system capability/physics to gain control
  - Don't look like network cyber attacks – often no malware

Threat Actor Intent:
Cause generator damage

Use remote access to push equipment into forbidden operating zones resulting in damage

Threat Actor Intent:
Cause centrifuge damage

Centrifuge overpressure

Prevent pressure relief

Compromise sensor to cause controller to overpressure

Prevent relief valves from opening damaging centrifuge

Government/industry ICS security gaps

- CISA/NSA “Know your opponent”, Shields-up”, etc.
- NIST
- TSA pipeline cyber security requirements
- EPA cyber security requirements
- CMMA
- NERC CIP/AWWA/API/AGA
- FDA Food Security Management Act
- ICS 706-02 (DOD)
- CVEs/CWAs
- Moody’s cyber heat map – electric, water, and gas Very High Risk

Government process sensor gaps

- ORNL, PNNL, NREL 2021 report on sensor issues in Buildings
  - Cybersecurity threats are increasing, and sensor data delivery could be hacked as a result. How hacked sensor data affects building control performance must be understood. A typical situation could include sensor data being modified by hackers and sent to the control loops, resulting in extreme control actions. To the best of the authors' knowledge, no such study has examined this challenge.
- March 16, 2022, NIST Special Publication 1800-10
  - NIST acknowledged many device cybersecurity capabilities may not be available in modern sensors and actuators

MCCS Cybersecurity

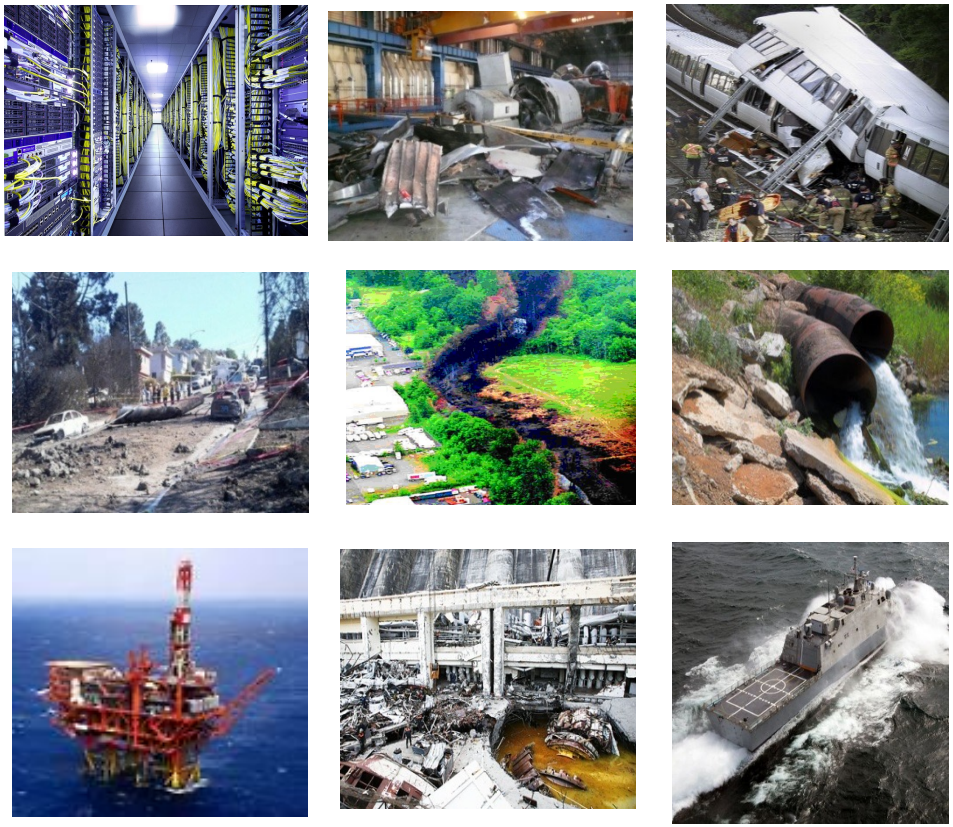
Strategic: Design & Build Cybersecure MCCSs

- IC Facilities Cybersecurity Standard (ICS 706-02)
- ICS 706-02 Technical Implementation Guide (v1.0 DRAFT)
- International Standards
  - ISA 62443 Multi-Part Standard, Security & Maturity Levels
  - ASHRAE – Secure Connect (BACNet Protocol)
- ISA Security Compliance Institute (ISCI)
  - ISA-SECURE Conformance Testing
- Zero Trust Architecture for MCCSs
  - White paper in development

Process sensors not addressed

Control system cyber incidents are real

- >11 Million incidents to date
  - Impacts ranged from significant discharges to significant equipment damage to major electric outages to deaths
    - >34,000 deaths to date
    - >$100 Billion in direct impacts
  - Contributed to bankruptcies
- Very few control system-specific cyber security technologies, training, and policies
  - Lack of appropriate forensics
- >2 million control system devices directly connected to the Internet (and counting)
  - Many are gateways
- Resilience and recovery need to be addressed



No information sharing on cyber incidents
Information not used in design or training

Example sensor-related incidents

- Stuxnet
- Airplane crashes from erroneous sensor readings (Boeing and Airbus)
- Dam failure from erroneous sensor readings releasing billions of gallons of water
- Sensor malfunction resulted in the release of 10 million gallons of untreated wastewater
- Pressure transmitter sensing line clogged tripping multi-unit power plant
- Safety relief valve in a nuclear plant did not lift because the pressure sensor never reached its setpoint
- Voltage sensor failure in power plant in Florida caused a 200MW load swing that caused a 50MW load swing in New England
- IOT sensor failure compromises lab building
- Tank farm explosions from erroneous level sensing
- Refinery explosion from sensor failures

Electric industry cyber-related issues

- >500 control system cyber incidents
  - 6 cyber-related outages affected >96,000 customers
  - Utility SCADA system targeted, compromised, and shutdown for 2 weeks
- Per DOE OE 417,
  - 37 cyberattacks, 4 >1/ 1/2half days, 1 >4 months
  - 150 incidents with complete loss of view and control >30 minutes
    - 11 with demand losses of >80MW
    - 4 started and stopped at the exact same time
- No encryption in protective relay communication protocols
- Russia and China have attacked US electric grid
  - Large Chinese transformers with hardware backdoors, other attacks
  - Russian malware in US electric grids since 2014, other attacks

Selected electric cyber incidents

- Case 1
  - Utility pen tested data center
  - Used same pen test software in substations, without testing
  - Shot down relay communications to 400 230 and 500 KV relays
  - Originally appeared to be Industroyer, SCADA not aware of relay comms lost
- Case 2
  - Utility ordered new distribution SCADA
    - Load shed algorithm to be manual
  - SCADA delivered (with factory and site acceptance testing)
  - SCADA operator thinking load shed was manual selected load shed
  - 400 MW of load shed affecting 96,000 customers

Recent case (identified 9/28/22)

- An antivirus software engine on EMS production servers had a flaw that caused affected servers to become unresponsive.
- The flaw was not recognized in the patch testing.
- Two separate events over the span of two weekends led to a period of 31 consecutive minutes of complete loss of EMS functionality; this occurred again on the following Saturday for a period of 81 consecutive minutes. These performance degradation events removed the ability to control BES elements at the impacted substations.

Suspect equipment from China

- DNI's National Intelligence Council's National Intelligence Estimate:

"China is the world's leading supplier of advanced grid components for ultra-high-voltage systems, such as transformers, circuit breakers, and inverters, **which we assess creates cyber vulnerability risks**."

  - Compromising circuit breakers can initiate Aurora
  - Inverters are used to convert AC to DC. Inverters are used in roof top solar panels, swimming pool pumps, electric grids, power generation, water/wastewater, manufacturing, etc. The U.S. has imported 170,796,103 inverters from China since 2002 (5 million in 2021)

- Logic bombs in Digital Fault Recorders

Counterfeit Chinese parts

- Load Tap Changer (LTC) “knock-off” in a Chinese transformer
  - Can cause transformer damage
  - Can cause injuries
  - Can impact load balancing
  - “Real” LTC used by many non-Chinese transformer vendors
- Counterfeit transmitters
  - Measures, pressure, level, flow, temperature – Can directly affect safety
  - Affects many process sensor vendors
  - Counterfeit transmitters available on Amazon, eBay, elsewhere

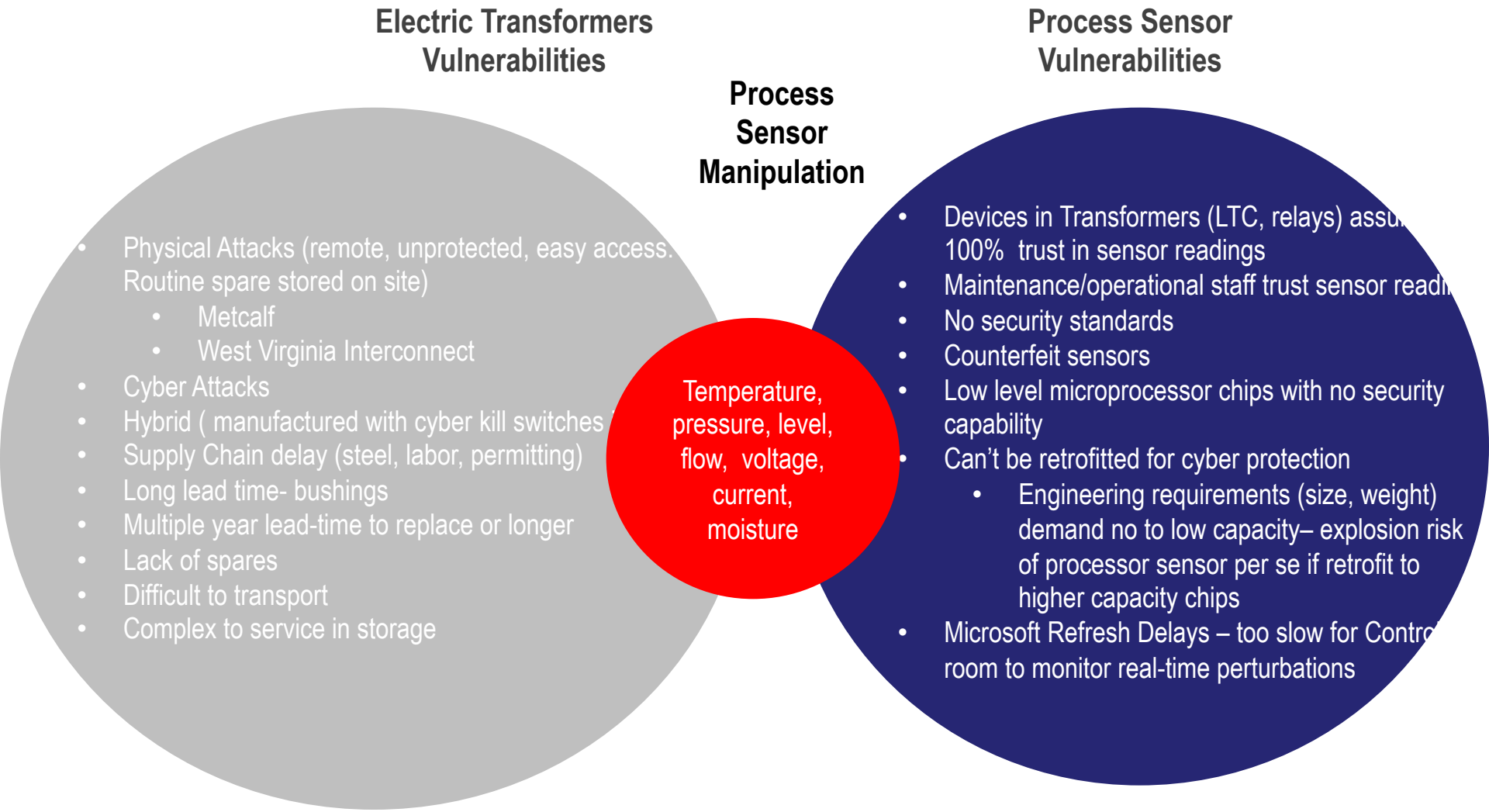
Internal/External

SALES NEWS

Product Service Announcement – Counterfeit Transmitters

We have become aware of a number of instances in which counterfeit field instruments, bearing the Yokogawa logo, have reached some of our customers. At first glance, they are nearly indistinguishable with a semblance of functionality and interface that mimics our product. A thorough investigation has confirmed that these counterfeit instruments are being produced by **unauthorized manufacturers** in China who have gone to great lengths to imitate Yokogawa products. Performance test results show that they are severely inferior in quality, and performance and they pose a **serious safety risk**. It is important to note that these counterfeit instruments carry tagging that indicates they are conformant, but they **are not conformant for use in ExD and other hazardous areas.** They also do not meet the stringent engineering and manufacturing requirements observed by FM and other regulatory bodies.

Transformers can be attacked by process sensors



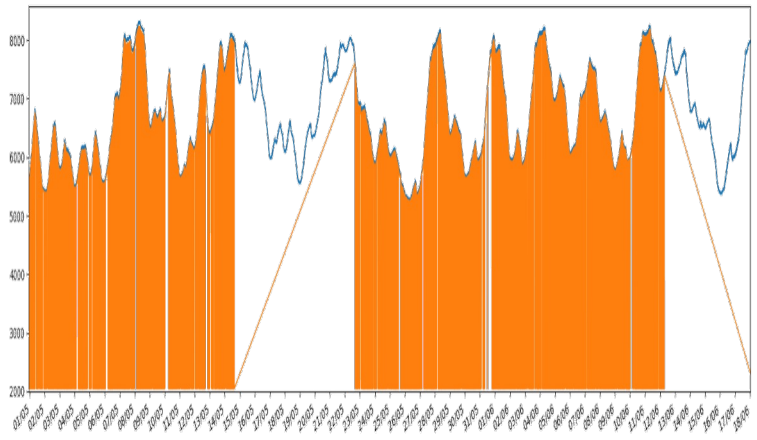
Renewable issues

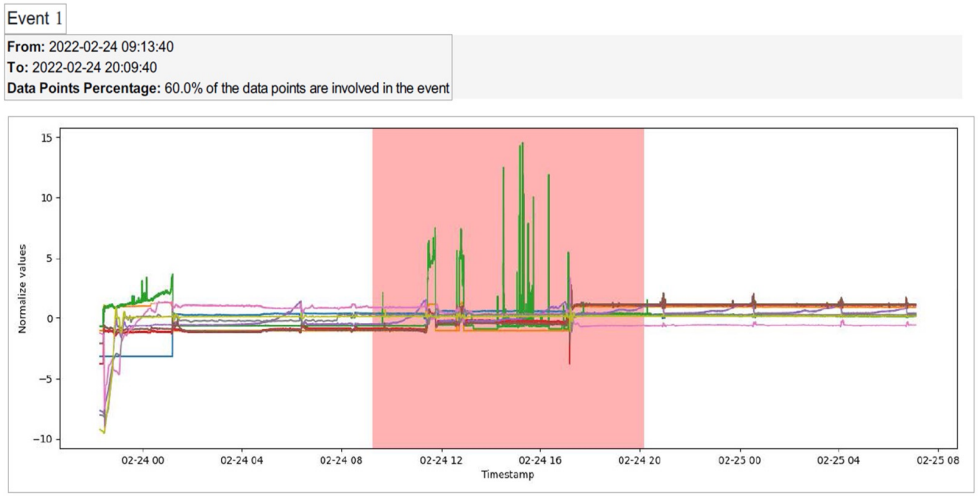
- Solar – inverters
  - Inverters can be compromised by programming, sensors, or supply chain
  - Inverter-based resources can ramp up and down much more quickly than a conventional power plant, that can lead to tripping events
    - June 2021 inverter-based tripping event involving 14 solar facilities and a loss of 1,666 MW
- Wind - turbines
  - Depend on process sensors
  - Includes many systems common to gas and steam turbines including lubrications systems
  - Susceptible to Aurora attacks

What does this mean to the Navy

- Navy has facilities, planes, ships, data centers
  - Have similar equipment and suppliers
  - Ships are “power plants with rudders”
  - Compromised sensors affect reliability and availability of facilities
- In US, Navy depends on the “public” grid, but installing microgrids
- Overseas, Navy may operate their own grids

Silver lining - Improve security and performance





Off-line sensor monitoring is unaffected by any routable network issues including ransomware - water

Sensor monitoring identifies process impacts not seen with conventional monitoring or the HMI – metals

November issue of IEEE Computer

What needs to be done

- Create an environment to overcome the Engineering/Networking cultural gap
- Government, regulators, and industry organizations need to address legacy field devices
  - **Develop Level 0,1 training for university students, existing work force, and decision makers**
- Develop appropriate standards for legacy field devices
- Develop cyber forensics for legacy Level 0,1 devices
- Monitor process sensors at the “physics” level
- Develop next generation field devices with built-in security
- Consider “cloaking” the systems

Joe Weiss
Applied Control Solutions, LLC
joe.weiss@realtimeacs.com
(408) 253-7934
www.controlglobal.com/unfettered