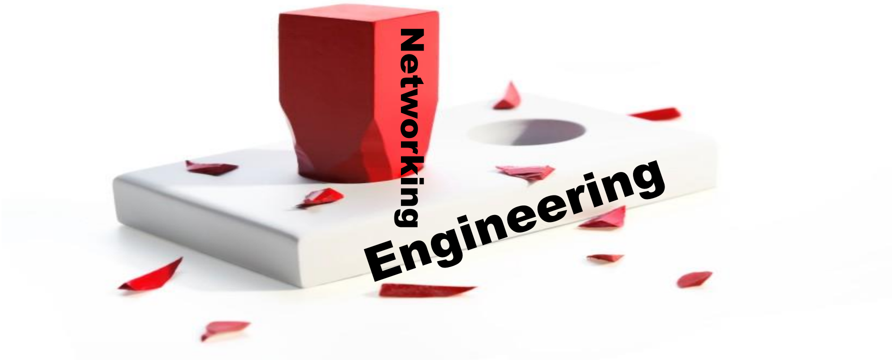
# IoT, IIoT, and supply chain implications in OT and process sensor cyber security

## April 19, 2023

## Presentation to

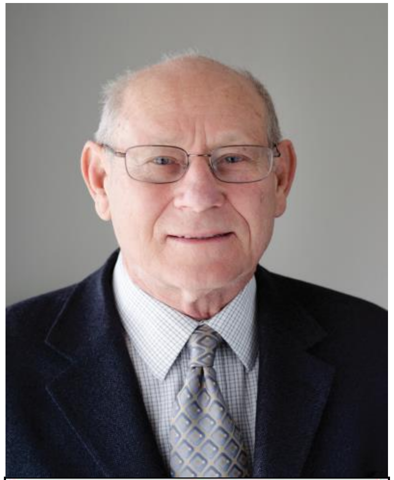
## IOT Advisory Board

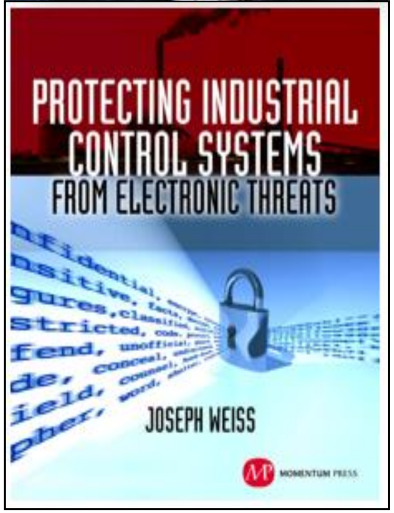
Joe Weiss  PE, CISM, CRISC, ISA Fellow
Managing Partner
Applied Control Solutions, LLC
joe.weiss@realtimeac



# 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

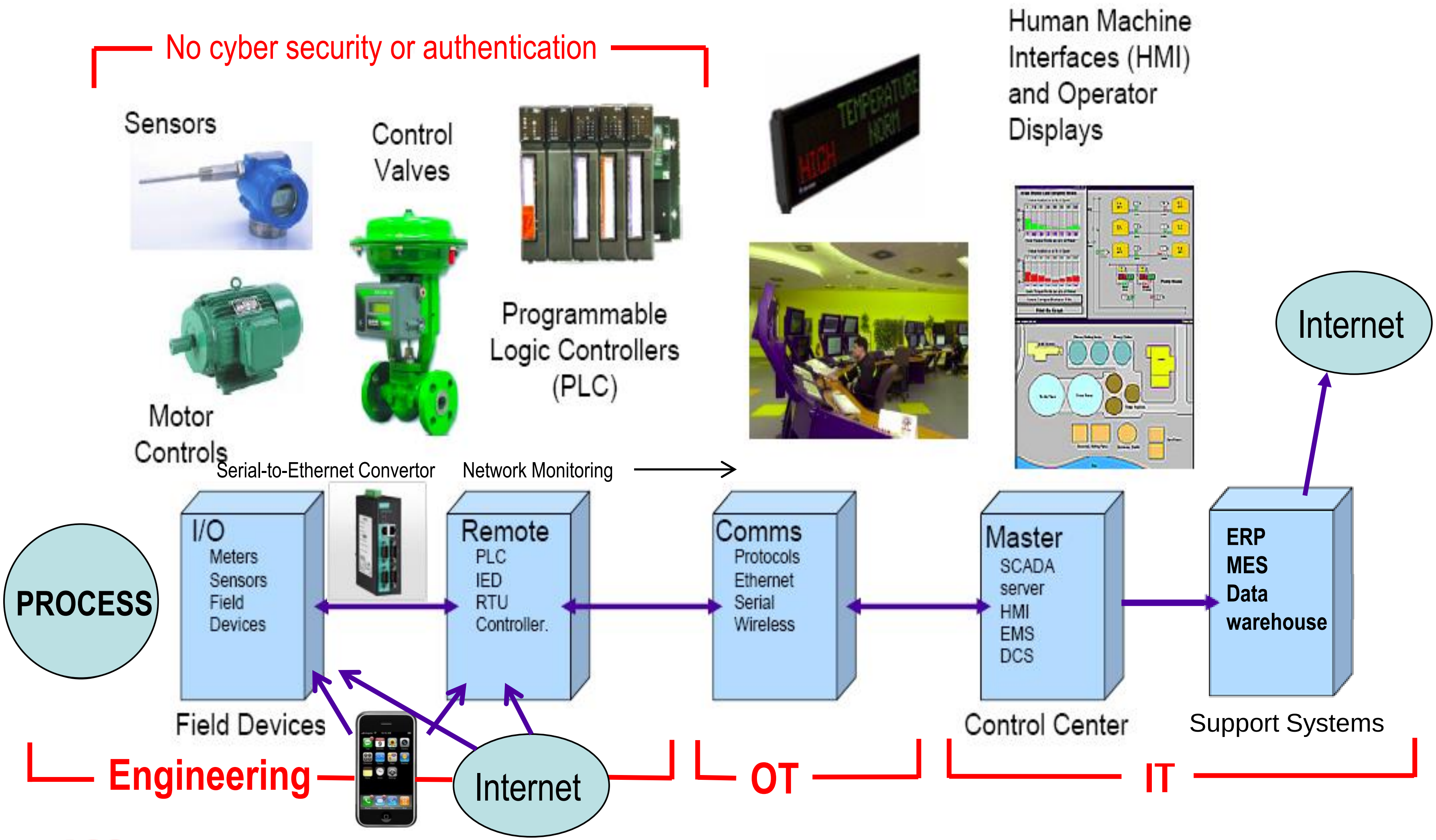




# Meeting observations

- Focus on networks not devices
- Process sensors not addressed
  - Process sensors are used in all infrastructures, Smart Cities, …
  - Process sensors needed for sustainability, safety, reliability, …
  - Process sensors have no cyber security
  - Don’t have alternatives for secure process sensors
- Counterfeit parts (sensors) is a problem

# Control system basics



No cyber security or authentication

Sensors

Control Valves

Programmable Logic Controllers (PLC)

Human Machine Interfaces (HMI) and Operator Displays

Motor Controls

Serial-to-Ethernet Convertor

Network Monitoring

PROCESS

I/O
Meters
Sensors
Field
Devices

Remote
PLC
IED
RTU
Controller.

Comms
Protocols
Ethernet
Serial
Wireless

Master
SCADA
server
HMI
EMS
DCS

ERP
MES
Data
warehouse

Internet

Field Devices

Control Center

Support Systems

Engineering

Internet

OT

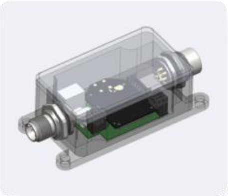
IT

# IoT, IIoT, and Process Sensors

- IoT – “Fitbits and refrigerators”
  - For consumers and non-critical applications
  - Inexpensive with no real-time control or safety
- IIoT – Industrial/manufacturing data acquisition
  - For data analysts
  - Inexpensive, often wireless, for big data analytics
  - No real-time control or safety
- Industrial process sensors – “power plants and pipelines”
  - For control and safety
  - Expensive with specific real-time control and safety requirements
  - No capability to add additional security

- Perimeter cameras

- Equipment monitoring



- Process control and safety

# Process sensors - where you go “boom in the night”

- No passwords, antivirus, authentication, keys
- Don’t use Windows
- Use insecure sensor networks (HART*, Profibus, etc.)
- No cyber certification, Factory Acceptance Test, or Site Acceptance Test criteria
- Technologically incapable of being cyber secured
- 100% trust

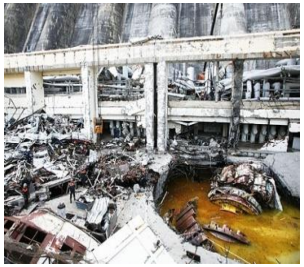
* Highway Addressable Remote Transducer

# Control system cyber incidents are real

- >17 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 to be addressed

**No information sharing on cyber incidents**

**Information not used in design or training**



ACS APPLIEDCONTROLSolutions

# Example Process Sensor Cyber Incidents

- Airplane crashes from erroneous sensor readings (>1,000 deaths)
- Dam failure from erroneous water level readings
- Sensor error released millions of gallons of untreated wastewater
- Sensor error in Florida power plant caused load swing in New England
- Refinery and chemical plant explosions from sensor issues
- Tank farm explosions from sensor issues
- …

# Need to address process sensors

- GAO report - Critical Infrastructure Actions Needed to Better Secure Internet-Connected Devices (GAO-23-105327)
  - Process sensors not addressed
- NIST Special Publication 1800-10 Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector, March 16, 2022
  - **"It is acknowledged that many of the device cybersecurity capabilities may not be available in modern sensors and actuators"**
- PNNL, ORNL, 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.**
- CISA guidance
  - Process sensors not addressed

# Sensor security issues not well understood

- From an acknowledged process industry instrumentation expert: *"I have spent years talking to brick walls and brick heads about the lack of security in field devices. Their response is typically that they are air gapped and that everything is safe and secure. Irrational fantasy at best. I am not alone in this quest, but I am definitely in a minority."*

# Sensor monitoring case history

- Facility felt existing process sensors and HMI's not reflecting actual plant productivity – not cyber concerns
- Selected a typical line for testing – multiple process sensors, pumps, motors, drives, and valves
  - 16 sensors – Pressure, Temperature, Flow, Motor amperage, vibration, valve position
- Monitored physics – 4-20 milliamp currents with machine learning

- Identified problems not seen from Windows HMI including inoperable sensors and pump operational issues

- Identified 3% hit on net productivity in billion-dollar facility

- Could have an affect on credit ratings

# Key project findings

- Not a cyber security project
  - Substantial plant participation
- Sensors not as accurate as thought
  - Cyber incidents not identified
- Windows can be misleading
  - Too much trust and cyber security focus
- Significant information “buried” in the process sensors
  - Maintenance, tuning, calibration,…
- Real ROI when address control systems
  - Improved productivity and cyber security “comes along for the ride”

# Recommendations

- Process sensors are cyber vulnerable and have caused cyber-related catastrophic failures
  - Extend cyber security requirements to include analog and digital process sensors and serial and point-to-point networks
  - Revise cyber security requirements from CISA, TSA, EPA, NERC/FERC, NRC, DOD, and others to include process sensors and their unique limitations
  - Include appropriate cyber security training for OT network personnel and engineers
  - Involve engineering organizations
  - Monitor “physics” of the sensors
    - ROI comes from improved operations, maintenance, product quality, and process safety

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