Joseph Weiss PE, CISM, CRISC
Managing Partner Applied Control Solutions
Managing Director ISA Nuclear Plant Standards, Fossil Plant Standards, Control System Cyber Security
(408) 253-7934
Email: joe.weiss@realtimeacs.com
Web: www.realtimeacs.com/unfettered

Comments of Joseph Weiss to the Secretary of Energy's Advisory Board, October 28, 2021

My background
I am an independent consultant specializing in cyber security of industrial control systems used throughout all industries, manufacturing, buildings, transportation, and defense. I have been involved in instrumentation, control systems, and equipment diagnostics for almost 50 years and cyber security of control systems since I helped start the control system cyber security program for the electric industry while at the Electric Power Research Institute (EPRI) in 2000. I helped the Idaho National Laboratory (INL) start the INL SCADA Test Bed, and supported NIST in extending SP800-53 for control systems, supported FERC, the National Association of Water Companies, the National Academies Federal Facilities Council on cyber security for federal buildings, the February 2021 NNSA 5G and Nuclear Nonproliferation Workshop, and the International Atomic Energy Agency. I am the Managing Director of the International Society of Automation (ISA) Nuclear Plant Standards (ISA67), Fossil Plant Standards (ISA77), and Industrial Automation and Control System Standards (ISA99). I also wrote the first book on consequence-based engineering for control system cyber security in 2010 – Protecting Industrial Control Systems from Electronic Threats. Consequence-based engineering means determining what impacts can, and have, occurred and reducing risk by design, training, and procedures.

Process sensors
Process sensors measure pressure, level, flow (e.g., steam, liquids, electric power, etc.), temperature, voltage, current, etc. These devices are essential for cyber security, process safety, reliability, product quality, and resilience by providing critical input to field controllers, actuators, motors, drives, analyzers, robots, and Windows-based operator stations. All organizations that monitor or control physical processes utilize similar types of process sensors from common vendors with common cyber limitations. *That includes DOE's operating portfolio of commercial and military nuclear facilities, electric power generation including hydro and renewables, electric grids including microgrids, smart manufacturing, smart buildings, high-power usage devices including electric motors, etc.*

IT and Operational Technology (OT) cyber security practitioners take a network-based approach that monitors the Internet Protocol (IP) networks for network anomalies. This is necessary and sufficient for IT networks but is not sufficient for full control system cyber security. That is because process sensors, which are input to OT networks, have been wrongly assumed to be uncompromised, authenticated, have cyber logging capabilities, and provide correct readings throughout their operating cycle.

Erroneous process sensor readings, whether from unintentional or malicious causes, have contributed to major catastrophic impacts yet process safety standards do not address the cyber security of the process sensors. As a result, process sensor cyber vulnerabilities were examined in a joint ISA84 (process safety)/ISA99 (cyber security) assessment of a state-of-the-art safety pressure transmitter installed in a Liquified Natural Gas facility. The pressure transmitter failed 69 of the 138 individual cyber security requirements that could have prevented safe operation of the facility[1]. All infrastructures and equipment are at risk as the process sensors aren't secure and authenticated (that is, knowing the sensor measurement signal come from the sensor).

Control system cyber incidents are real
Our adversaries are aware of these limitations. An industrial security specialist for the Electric Industry of Iran has in-depth knowledge of industry control system security frameworks and best practices such as

[1] https://www.controlglobal.com/blogs/unfettered/ot-network-security-often-does-not-view-control-system-devices-and-the-process-as-their-problem

ISA-99/IEC-62443, NERC CIP, NIST 800-82, SANS security practices, Nozomi tools, and Siemens, Yokogawa, and ABB control systems.[2]

The Russians hacked the Triconex safety systems in a Saudi Arabian petrochemical plant (Triconex safety systems also are used in U.S. nuclear plants, petrochemical plants, and water systems). The intent of the hack was to blow the plant up. The hack wasn't detected even after the plant was shut down by the malware.[3] The lack of identifying control system cyber incidents directly impacts the ability to meet recent governmental actions on cyber security such as the TSA cyber security requirements and the Presidential Executive Order 14028.[4] Monitoring of the process sensors would help as the process sensors would provide direct indications of process anomalies regardless of cause.

The Chinese have provided counterfeit pressure sensors to the North American market[5] and installed hardware backdoors in large power transformers provided to US utilities[6]. The lack of process sensor authentication allows "spoofed" sensor signals to take control of the transformers.[7,8] As there is no authentication of the process sensor signals (are the sensor signals coming from within the transformer or "Beijing"), it is not possible to know if the transformers have been compromised.

Paradigm change

Neither IT nor OT networks can be fully protected from cyberattacks. Consequently, a paradigm change is needed to protect crucial infrastructures. My suggested approach is essentially "back-to-the-future" by monitoring the electrical characteristics of the process sensors out-of-band (not connected to any Internet networks) in real time. Engineers have used this approach for monitoring equipment health (process anomaly detection) for many years. Until recently, the approach was not applied to cyber security as the requisite machine learning wasn't available.

Out-of-band process sensor monitoring results in isolating the process sensor measurements from network malware whether coming from the IT or OT networks. This approach can help justify continued facility operation during ransomware attacks as the malware cannot reach the process sensor monitoring. Meanwhile the process sensor monitoring continues to provide a real-time status of the operations. Additionally, process sensor monitoring provides a predictive maintenance capability that improves productivity and safety. Others have recognized the value of this approach[9].

What DOE needs to do

- Encourage the paradigm change of monitoring the process sensors,
- Encourage cyber security training for the personnel responsible for process sensors,
- Coordinate with CISA and other government and industry experts to address process sensor issues.

---

[2] https://www.controlglobal.com/blogs/unfettered/iran-is-aware-of-electric-substation-cyber-threats-and-vulnerabilities

[3] https://www.controlglobal.com/blogs/unfettered/we-cant-detect-a-cyber-attack-that-trips-a-plant-but-we-immediately-identify-an-outage-as-not-being-a-cyber-attack

[4] https://www.controlglobal.com/blogs/unfettered/executive-order-14028-on-cybersecurity-does-not-adequately-protect-critical-infrastructures-real-cases-prove-it/

[5] https://www.controlglobal.com/blogs/unfettered/the-ultimate-control-system-cyber-security-nightmare-using-process-transmitters-as-trojan-horses/

[6] https://www.controlglobal.com/blogs/unfettered/presidential-executive-order-13920-was-not-due-to-a-malware-event-recent-and-upcoming-events-will-discuss-the-event/

[7] https://www.controlglobal.com/blogs/unfettered/formal-response-to-ferc-complaint-el21-99-000-on-chinese-equipment-in-the-us-grid

[8] https://youtu.be/x0EawFC18MI

[9] https://www.controlglobal.com/blogs/unfettered/us-critical-infrastructure-cyber-security-is-backwards-its-the-process-that-counts-not-the-data