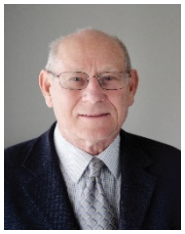
The Need to Change the Paradigm of Control System Cyber Security – Monitor Process Sensors

Joe Weiss, PE, CISM, CRISC, Applied Control Solutions, LLC
Rob Stephens, PhD, JDS Energy and Mining
Nadine Miller, ME, MBA, JDS Energy and Mining

Biographies



Joe Weiss is an expert on instrumentation, controls, and control system cyber security. He has published over 80 papers on instrumentation and control systems, control system cyber security, chapters on cyber security for Electric Power Substations Engineering and Securing Water and Wastewater Systems, coauthored Cyber Security Policy Guidebook and authored Protecting Industrial Control Systems from Electronic Threats. He has amassed a database of 12 million actual control system cyber incidents. He is an ISA Fellow, Managing Director of ISA99, a Ponemon Institute Fellow, and an IEEE Senior Member. He was featured in Richard Clarke and RP Eddy's book- Warning – Finding Cassandras to Stop Catastrophes. He has patents on instrumentation, control systems, and OT networks. He is a registered professional engineer in the State of California and has CISM and CRISC certifications.

Rob Stephens is a strategic thought leader, innovator, and entrepreneur in the mining and primary materials industries. Starting with a PhD in chemical and materials engineering focused on nanotechnology materials production, he works at the nexus of technology, innovation, and strategy. He is currently working on a comminution (breaking rocks) startup, a foundry for technology startups, and control system cyber security. His technical expertise ranges from ore body knowledge, minerals processing, metals smelting and refining, and advanced materials processing to environmental and climate change technologies. He strongly supports effective open innovation ecosystems through his continued involvement with the Canada Mining Innovation Council (CMIC) and professional societies.

Nadine Miller is the Vice President of Project Development at JDS Energy and Mining. Prior to joining JDS, she led the Business Development departments for two of the world's largest engineering consulting firms' Toronto Offices: Bantrel with the backing of Bantrel's parent company, Bechtel and SNC-Lavalin's Mining and Metallurgy. She is a professional engineer with over 20 years of experience in engineering design and project management in the mining and transportation industries. She also serves as an Independent Non-Executive Director for Wesdome Gold Mines and OMAI Gold Mines, both Canadian gold mining companies, and a Strategic Advisor at Awz Ventures Inc. (a venture capital fund) and Drone Delivery Canada. She graduated from the University of Oxford's Saïd School of Business with an MBA focused on finance and strategy, Massachusetts Institute of Technology (MIT) with a Masters degree in Civil and Environmental Engineering, and the University of Toronto with a Bachelor of Applied Science degree.

1 Executive Summary

With the never-ending, and too often successful, attacks on critical infrastructure networks, there needs to be a better way to protect control systems and the processes they monitor and control. On July 28, 2021, an announcement was made about the President's Industrial Control System Cybersecurity (ICS) Initiative to facilitate the deployment of technology and systems that provide threat visibility, indicators, detections, and warnings. To date, this is a network-based approach specific to cyber threats. However, the existing approach of securing critical infrastructures by securing the networks alone is inadequate without being able to verify the process sensor measurement integrity (process anomaly detection). As an example, the ISA99 control system cyber security standards, like all other cyber security standards, assume process measurement integrity, without requiring assurance of process measurement integrity like is required for data. Assuring process measurement integrity provides predictive maintenance and process integrity as well as validity of the sensor input for cyber security. The Israel Water Authority recognized the need to monitor the sensor signals and is monitoring the electrical characteristics of the process sensors as the process sensors are ground truth and not susceptible to network attacks so long as the raw signals can be measured before any signal pre-processing occurs. Process sensor monitoring needs to be incorporated into the overall control system cyber security program to complement the network monitoring approaches. The US government, insurance companies, credit rating agencies, and others need to recognize what really needs to be secured – the field control system equipment that keeps lights on and water flowing.

2 Introduction

Modern control systems, based on process sensors feeding into programmable controllers that direct actuators to make intended actions, are ubiquitous in our modern world. They enable breakthroughs in safety and environmental performance as well as optimization, enhanced reliability, and automation leading to improved productivity. However, they are also capable of being accidentally or maliciously compromised in cyber incidents. If control systems are affected by a cyber incident, whether unintentional or a deliberate attack, the benefits brought to critical infrastructure, industrial and manufacturing processes, and transportation systems by modern control systems can be seriously impacted. In worst cases, cyber incidents have killed people, caused serious environmental damage, inflicted serious economic harm, and caused geopolitical conflict [1].

At its most basic level, control system cyber security is about keeping lights on, water flowing, industrial and manufacturing processes operating as intended, and robots, including autonomous vehicles, serving humanity. However, control system cyber security can also have national security and economic implications. A cyber incident causing damage to a large fraction of a nation's electrical infrastructure could devastate a nation's economy for years as long-term replacement equipment is sourced and installed (assuming sources are available). A cyber incident involving a modern airliner with fly-by-wire controls or autonomous vehicles could ground the entire fleets for months as root causes are identified and protective fixes applied.

Modern control systems rely on Operational Technology (OT) Internet Protocol (IP)-based networks to bring significant safety, environmental, productivity, and governance improvements. However, along with these improvements come significant cyber vulnerabilities.

The fallacy about critical infrastructure cyber security is the thinking that IP networks are needed to keep lights on, water flowing, and industrial processes and transportation systems operating. For more

than 80 years, the electricity grid operated without IP networks. Control devices in power systems are designed to work in coordination with each other so the equipment can work with or without the Supervisory Control and Data Acquisition (SCADA) networks although the SCADA network significantly improves productivity. Following the 2015 cyberattack of the Ukrainian power grid, the Ukrainians continued to operate the grid manually for months without the IP networks as the IP networks couldn't be trusted to be free of malware. More operator intervention was needed, and productivity was lower, but the lights stayed on and the economy continued to function. However, the grid could not be operated if the critical hardware were compromised or damaged. This includes the process sensors monitoring and controlling the grid as well as the generators, transformers, and switchgear.

July 28, 2021, an announcement was made about President Biden's Industrial Control System (ICS) Cybersecurity Initiative [2], which is a voluntary, collaborative effort between the federal government and the critical infrastructure community to facilitate the deployment of technology and systems that provide threat visibility, indicators, detections, and warnings. To date, this is a network-based approach specific to cyber threats. On the other hand, control system field devices such as pressure, level, flow, temperature, and voltage sensors (often not considered part of OT) are inherently insecure and generally not designed to be connected to IP networks. The introduction of smart sensors and transmitters as well as wireless transmitters are introducing a wide range of new cyber security vulnerabilities. The President's ICS Initiative is not addressing this problem.

Others, however, have recognized this problem and what they are doing may hold useful lessons for the US. In particular, **the Israel Water Authority recently selected off-line, out-of-band process sensor monitoring technology as a key component to help secure the country's water systems, making control system cyber security about the process and not just the data** [3]**.** The US would do well to reconsider its approach to securing critical infrastructures: networks and data should of course be secured, but that's a necessary and not sufficient condition to securing infrastructure.

3 Background

Prior to 2000 and particularly after the 9/11 event, cyber security was simply one of the risks that had to be considered when designing and implementing control systems along with seismic risk, environmental risk, fire risk, reliability risk, etc. Those risks were regarded as engineering considerations and managing them was considered an engineering function. The intent was to ensure that the engineering basis of the design would be met, regardless of the risk. Consequently, engineering organizations were responsible for cyber security. It was a "bottom up" approach of process anomaly detection, performed in the interest of mission assurance. For example, this was the basis of the Electric Power Research Institute' (EPRI's) control system cyber security program developed in 2000. Unfortunately, this program is now, like others, about securing the networks.

Sometime after 9/11, cyber security evolved to became part of national security. However, around the same time, cyber security for control systems was moved to the IT (now OT) network monitoring organizations with engineering no longer involved. As a result, control system cyber security went from Mission Assurance to Information Assurance**.** The focus on networks rather than on the process can also be seen by having the CISO and not the Vice President of Engineering/Operations responsible for the cyber security of control systems [4]. IT specialists understand networks and business computers. However, network specialists do not have a deep understanding of the physical, chemical, and electrochemical processes and systems, including the sensors and actuators, nor the process and system dynamics the way process control, electrical, and mechatronics engineers do.

Consequently, cyber security monitoring and mitigation tended to move to the IP network layer where IT specialists are comfortable with their existing knowledge – network anomaly detection tended to replace process anomaly detection. Engineers are also not explicitly taught about cyber security and IP networks so they have limited ability to meaningfully interact with the IT specialists assuming that the IT specialists actually recognize their lack of required knowledge and seek involvement of those with complimentary knowledge. This lack of overlapping knowledge is shown graphically in Figure 1.

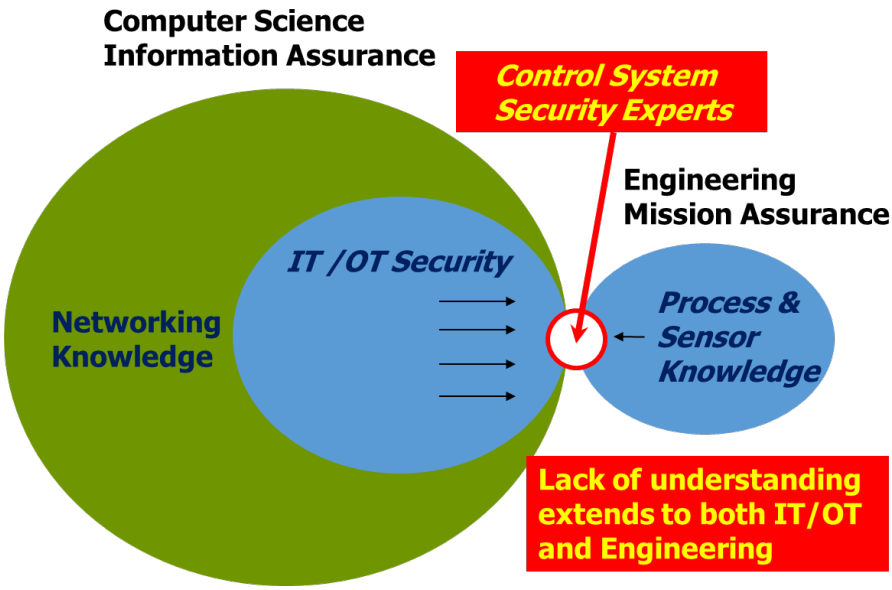


Figure 1: Control system cyber security knowledge gap

The reticence of the US government and the broad industry segments to move away from a traditional network-based approach can be seen from the following examples:

- The July 2021 Version 2.0 of the Cybersecurity Capability Maturity Model (C2M2) [5] does not address the process sensors and process anomaly detection. How mature can the process be if it doesn't address what keeps the lights on and water flowing?
- The electric industry's North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cyber security standards consider process sensors out-of-scope for cyber security considerations.
- The recent podcast by Idaho National Laboratory personnel supports the network approach [6].
- Presidential Executive Order (EO)13920 [7] was issued following discovery of hardware backdoors in large Chinese-made electric transformers. As can be seen from the EO, it was focused exclusively on hardware and control systems. However, the government and industry responses were to turn this hardware attack into a software supply chain problem.

4 Use of sensor monitoring

Control system devices such as electrical system protective relays work on instructions entered into registers within the hardware of the device. These instructions reference other instructions and raw process sensor input data to perform desired commands. This means that devices such as protective relays have little to do with traditional higher-level networks but depend on the integrity of the sensors.

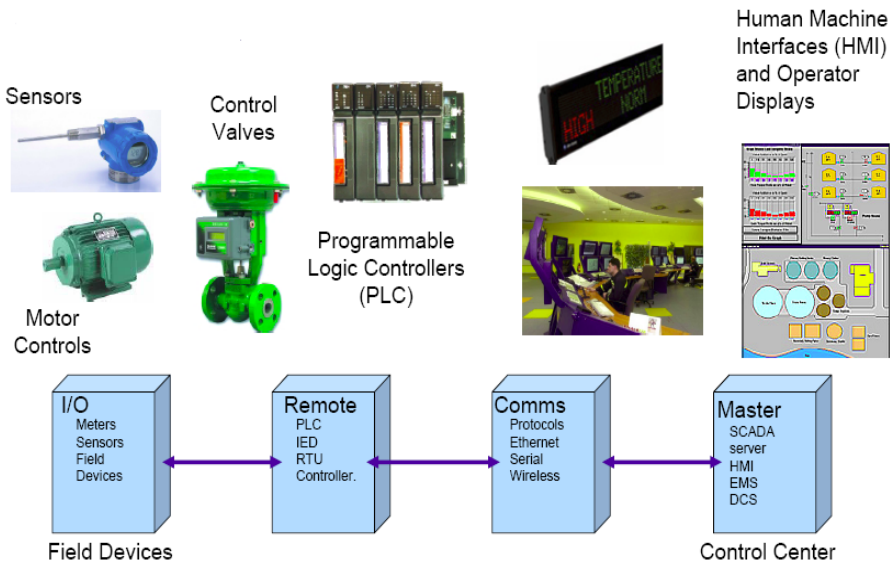


Figure 2: Control system architecture and components

The sensors are the windows that allow us to see into the process or system, and process sensor monitoring has been used for many years for process anomaly detection.

Legacy engineering field devices such process sensors, actuators, drives, positioners, and analyzers as shown in Figure 2 have no cyber security, authentication, or cyber logging nor can they be easily upgraded for cyber security.

Yet, process sensors deliver the inputs to the OT network **where the OT network monitoring providers ASSUME the sensor input is uncompromised, authenticated, and correct**. As noted previously, the introduction of smart sensors and transmitters as well as wireless transmitters introduce a series of new cyber security vulnerabilities. Because the sensor input is not authenticated, it is not clear that the apparent sensor data is actually coming from the sensors and not from "spoofed" signals. The controllers receiving the sensor signals have no way to authenticate the origin of the sensor signals and therefore automatically accept the sensor input and respond accordingly (a 100% trust model as opposed to the new zero trust cyber security model). Similarly, the responses of the actuators and drives, which occur in real time, assume the sensor inputs are authenticated (process sensor signals are actually coming from the sensors, not spoofed) and correct (accept the sensor input as correct if the signal isn't out of range).

This could be the approach the Chinese are using with the hardware backdoors in large electric transformers to take control of the transformers without having to hack into the IP networks. Therefore, there is a need to take an intractable network monitoring approach and make it a tractable engineering problem.

Modern Machine Learning (ML) algorithms enable pattern detection of the raw process sensor and actuator feedback signals that was not previously possible. It is this additional capability that enables sensor monitoring to identify process anomalies regardless of cause and independent of IP networks and their associated cyber vulnerabilities. It is acknowledged that not all process anomalies are caused by cyber incidents. However, working together, the IT specialists and engineers can pull out their

respective toolboxes and identify root causes that may include cyber-related causes. In this way, cyber incidents have a much higher probability of detection and appropriate response.

As a result, **the Israel Water Authority recently took the engineering approach and approved off-line, out-of-band process sensor monitoring technology to secure the country's water systems.** Unlike the prevalent US practice of monitoring IT and OT networks for cyber security (that is, for network anomaly detection), the Israeli approach is based on monitoring the electrical characteristics of the process sensors (process anomaly detection) and not just relying on network monitoring like the US.

5 Benefits of off-line sensor monitoring

The benefits of the Israeli approach include [8]:

- Raw process sensor signals provide ground truth about the physical operation of the system. Note that this assumes the use of 4-20 milli-amp analog sensors and smart digital transmitters if the raw process sensor signals can be obtained before any signal processing has occurred.
- The process sensor monitoring system is not susceptible to IT or OT unintentional network issues, or network attacks (including ransomware) or vulnerabilities induced by patch management oversights. In some cases, such as a ransomware attack, it will be possible to continue to operate the process or system in a manual or semi-automatic mode with confirmation from the sensor monitoring system that the process or system is responding as expected.
- As process anomaly detection, the system detects any anomaly regardless of cause, not just malicious cyberattacks, which means even sophisticated attacks that look like equipment malfunctions will be identified (e.g., Stuxnet).
- By monitoring in real-time, the system is essentially a sensor health monitoring system and so also functions as a predictive maintenance system that can be used to extend maintenance intervals for sensors and transmitters.
- According to Offshore Reliability Database, "42% of Safety Integrated Systems (SIS) dangerous failure modes come from process sensors (Figure 3). More modern technologies have made advancements to eliminate many of these traditional challenges by improving the robustness and *smartness* of these devices." It is the "smartness" meant to provide diagnostics that can induce additional cyber security vulnerabilities.
- Monitoring for sensor drift can be used to improve the accuracy of digital twins, which inherently assume that sensors are correct.
- Process sensor monitoring systems have detected equipment impacts that were not identified by the Windows-based OT monitoring system because of the increased sampling frequency possible with the process sensor monitoring systems.
- Monitoring the sensors requires the involvement of the engineers responsible for the process as not all anomalies are due to cyber incidents.
- Monitoring the process sensors provides authentication, which otherwise would not exist.
- The process sensor monitoring system is applicable to any critical infrastructure and has been installed in water, power, chemicals, and building controls. The concept can be applied more broadly to any control system with further development work.
- Monitoring of process sensors applies to all infrastructures as they all use process sensing. There is a limited number of fundamental parameters being sensed (pressure, temperature, flow, composition, voltage, current, frequency, etc.) but real knowledge comes from how the measurements relate to the process or system and this knowledge resides in the engineers and not the IT specialists.

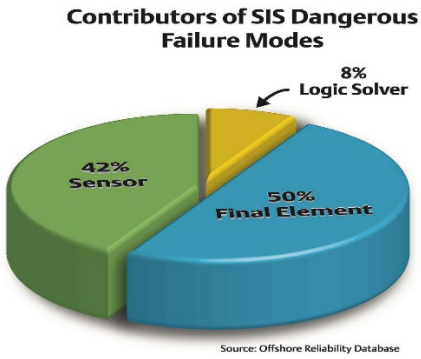


Figure 3: Process sensor contribution to SIS failure modes

This approach of addressing multiple industries meets the intent of the President's ICS Cybersecurity Initiative. The new TSA cyber security requirements do not address potential pipe failures because they are network-based and don't address the process sensors. As an example, critical pipeline operators have reported more than 220 cyber security incidents since the US Transportation Security Administration (TSA) implemented emergency measures in the wake of the crippling Colonial Pipeline's ransomware attack, according to US TSA Administrator David Pekoske [9]. However, there have no reports of pipeline product delivery upsets, spills, ruptures, or pipeline outages – the reports are of IT issues not affecting the operation of the pipelines. Sensor monitoring can be applied to the electric sector for situations like the hardware backdoors in the Chinese-made electric transformers to know that the sensing input going to the transformer devices are not "spoofed" signals coming from elsewhere. This approach can help any industry justify continued operation even with ransomware in the IT networks as there is a view of the plant processes. The list goes on.

6 The limits of network security

The disadvantages of the current US approach include:

- Neither IT nor OT networks provide ground truth about the process network and the sensor input is assumed to be uncompromised, authenticated, and correct. While network security is a key component of an overall cyber security system, it is not sufficient by itself if the sensor signal integrity cannot be confirmed. The emergence of "smart" sensors and transmitters significantly increases the risk associated with not being able to verify the sensor signal integrity.
- Network monitoring is a never-ending "whack-a-mole" issue (e.g., defenders come up with a solution, attackers come up with a bypass).
- Even the best network cyber security can be defeated (see SolarWinds).
- OT networks are susceptible to unsophisticated as well as sophisticated network vulnerabilities.
- OT organizations tend to exclude the engineers responsible for the design and operation of the control systems and equipment and plant processes.

7 References

[1] Protecting Industrial Control Systems from Electronic Threats, Joseph Weiss, Momentum Press, 2010.

[2] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[3] Israel Water Authority taps SIGA for cyber protection of the country's water supply, July 21, 2021, https://www.startuphub.ai/israel-water-authority-taps-siga-for-cyber-protection-of-the-countrys-water-supply/

[4] Attention Policymakers: Cybersecurity is more than an IT issue, PE, The Magazine for Professional Engineers, May/June 2020.

[5] US Department of Energy Cybersecurity Capability Maturity Model (c2m2), July 2021, https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[6] https://www.synack.com/were-in-synack-podcast/?utm_source=organic_social

[7] Securing the US Bulk-Power System US Presidential Executive Order 13920, May 1, 2020., https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system

[8] Changing the Paradigm of Control System Cyber Security - Monitoring Process Sensor Health, Texas A&M Instrumentation and Automation Symposium, January 2019.

[9] Critical pipelines have reported more than 220 cyber incidents since May TSA directive, July 27, 2021, https://www.cnn.com/2021/07/27/politics/pipeline-companies-reported-incidents-tsa-directive/index.html