Changing the Paradigm of Control System Cybersecurity

Joseph Weiss, Applied Control Solutions, LLC

Rob Stephens and Nadine Miller, JDS Energy and Mining

Current cybersecurity protection relies on network monitoring. Changing the paradigm to monitor process sensors makes it practical to develop workable control system cybersecurity engineering solutions while simultaneously addressing reliability, safety, resilience, and productivity concerns.

In the 1970s through approximately the mid-1990s, process sensors and control systems were isolated systems not connected to the outside world. They were entirely under the purview of the engineers that designed, operated, and maintained these systems. Consequently, the design and operational requirements were for performance and safety, not cybersecurity. The sensors and control systems provided engineering data useful only to the engineers. What changed wasn't the Internet but the microprocessor. The microprocessor allowed for the calculation and conversion capability to take 0s and 1s that weren't useful to anyone but the engineers and convert them to information that could be used by multiple establishments outside the engineering organization and even outside the corporate organization. It was the availability of this useful information that led the desire to be able to share this information within and outside

Digital Object Identifier 10.1109/MC.2021.3138231
Date of current version: 11 March 2022

0018-9162/22©2022IEEE

EDITOR **JAMES BRET MICHAEL**
IEEE Senior Member; bmichael@nps.edu

the immediate engineering facility. This enabled productivity improvements like just-in-time operation by sharing data with multiple organizations. The Internet and modern networking technologies were the vehicles for disseminating this valuable information.

Control systems utilize engineering devices and IT networks and network devices generally maintained by the IT department. IT has considered network cybersecurity to be important since the Morris worm in 1988 (https://www.fbi.gov/history/famous-cases/morris-worm). The control system community has been late to address the cybersecurity of control systems. Operations may be able to use IT for operational technology (OT) networks but not for the control system devices, which have no cybersecurity, authentication, or cyberlogging capabilities. The two communities have different goals and backgrounds, which have led to significant culture gaps that have not been overcome, even with "donut diplomacy."

Following 9/11, cyber became a first-class national security priority. At that time, the cybersecurity function for control systems was moved to the IT organization. Engineering was no longer involved. Consequently, cybersecurity monitoring and mitigation were at the Internet Protocol (IP) network layer—network anomaly detection. As a result, control system cybersecurity went from being mission assurance to information assurance. As the engineering systems were not included under IT's purview, the Purdue Reference Model Level-0,1 devices (see Figure 1) were not included in cybersecurity considerations. Note that level-0,1 devices are often referred to as *Industrial Internet of Things* devices.

These legacy engineering systems have no cybersecurity, authentication, or cyberlogging, nor can they be upgraded. The lower level sensor networks, such as Highway Addressable Remote Transducer (www.fieldcommgroup.org), Profibus (https://www.profibus.com/), and Fieldbus (https://www.fieldcommgroup.org/technologies/foundation-fieldbus), also have no cybersecurity. This lack of focus on control system devices is still occurring. This focus on OT networks has led to the second coming of

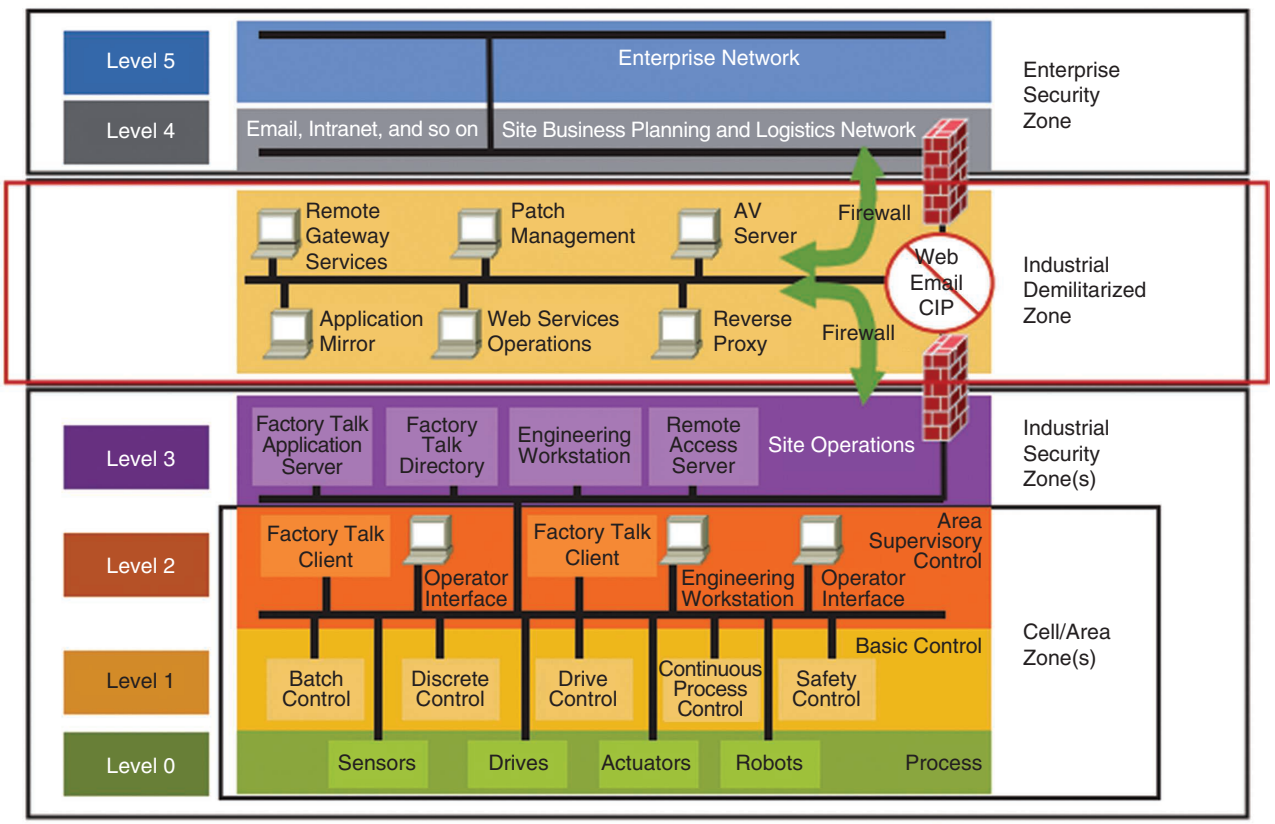

FIGURE 1. The Purdue Reference Model.[1] CIP: critical infrastructure protection.

the Maginot line (see Figure 2); that is, a disregard for any potential threat that was not IP network focused. As a colleague stated, "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." At least one nation state has used the approach of using hardware backdoors to bypass all cybersecurity protections, which led to the issuance of U.S. Presidential Executive Order 13920 (tps://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system). Authenticating the process sensor input within the transformers can help mitigate this problem.

FIGURE 2. (a) The Maginot wall and (b) OT cybersecurity (courtesy of Bob Radvanovsky and Joe Weiss).

CONTROL SYSTEMS

Instrumentation (process sensors) and control systems measure and control all physical processes. This includes energy, power, water/wastewater, pipelines, manufacturing, transportation, medical, defense, and so on. Control systems consist of process sensors connected to controllers, actuators, and human–machine interfaces (HMIs) (effectively, the control system network). The sensors and actuators operate almost exclusively in near real time (microseconds to milliseconds), whereas an HMI (operator display) provides operator information on the order of seconds to minutes. The sensors and actuators can operate, and in most cases were designed to function, without the IP network. Figure 3 provides a representation of the equipment and information flows in a typical process system from Purdue Reference Model Level 0 to the enterprise resource planning systems (Purdue Reference Model Level 4, as depicted in Figure 1).

Sensors are like the feelings in our fingers and toes; they provide the stimuli to our brains, which is the control system. If the sensing inputs to our brains are wrong for any reason, the actions of the brain will not be correct.

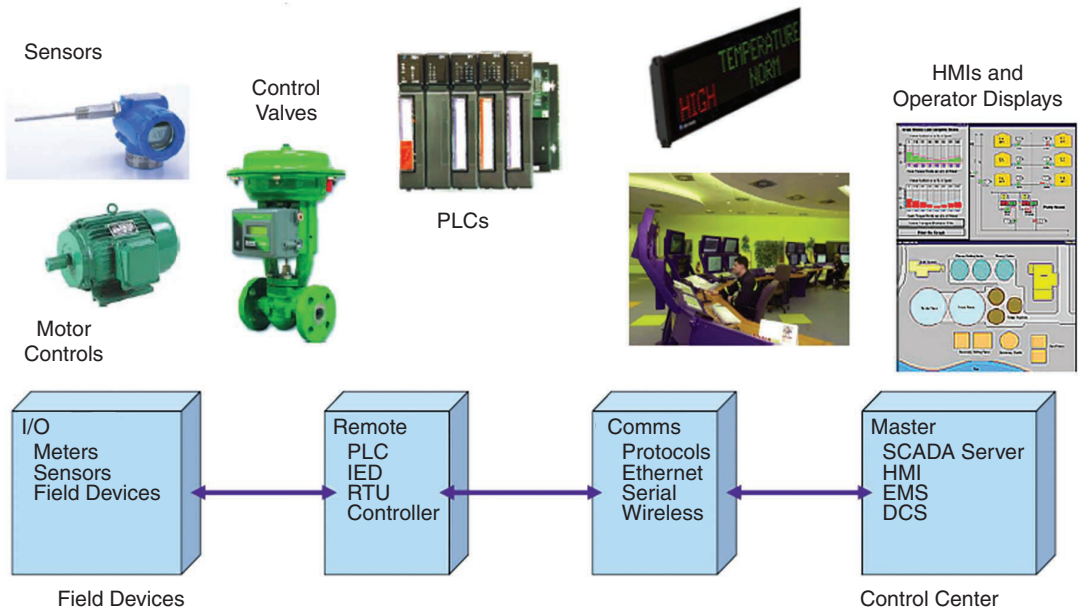

FIGURE 3. The control system loop (courtesy of Joe Weiss). I/O: input/output; SCADA: supervisory control and data acquisition; EMS: Expanded Memory Specification; PLCs: Programmable Logic Controllers; IED: intelligent electronic device; RTU: remote terminal unit; Comms: communications: DCS: distributed control system.

For example, if our fingers are insensitive to a flame near our fingers, the brain will not react to pull our fingers away from the flame. In the physical world, process sensors measure pressure, level, flow, temperature, voltage, current, strain, color, humidity, vibration, volume, chemistry, and so forth. The measurements start as analog stimuli and are then converted to digital signals and to Ethernet packets. These signals are input to control systems such as programmable logic controllers (PLCs) and electrical breakers, which are programmed to maintain systems within physical constraints based on sensor readings. The sensor signals are also the input to operator displays, generally Windows-based HMIs. The sensor readings are assumed to be stable and accurate. Consequently, calibration intervals are generally scheduled every one to three years to recorrect the sensor readings as they drift over time. The Internet of Things, Industry 4.0, smart grid, transactive energy, and so on all depend on reliable, accurate, and secure sensors, controllers, and actuators.

A simple way to view this problem is by comparing it to the home office shredder. If you continue to feed paper into the shredder, its temperature will increase until the temperature sensor reaches a safety limit, at which time the shredder ceases operation until the sensor returns to an acceptable operating temperature. No matter what you do, the shredder is useless until the sensor indicates the temperature is back to an acceptable level. This is essentially a safety interlock. Critical equipment such as turbines, motors, transformers, and protective relays have process sensors that act as safety interlocks to prevent the equipment from operating in unsafe conditions. The measured conditions can be that the temperature is too high, the flow is too low, the level is too high or low, the frequency is out of an acceptable range, and so forth. These process sensors have no cybersecurity nor authentication yet can be remotely accessed, either preventing equipment from starting or removing safety protection. Moreover, raw sensor signals are not monitored for reliability, safety, or security considerations, which is a major gap.

Regardless of how well communications are secured, if the sensors and actuators that constitute the ground truth of any industrial process are compromised or defective, it will not be possible to have a safe, reliable, or optimized process. The intent of the International Society of Automation (ISA) 84.09 (process safety/cybersecurity) effort was to determine the relative conformance and applicability of the ISA 62443-4-2[2] Component Specification's individual security requirements to the legacy (what is being built today as well those already installed in the field) digital safety pressure transmitter ecosystem, including the transmitters, host computers, field calibrators, and local sensor networks so as to determine what, if any, compensating measures might be necessary. The results were that most of the requirements in ISA 62443-4-2, including the fundamental cybersecurity requirements, could not be met. A number of the requirements, such as providing for a secure boot, could be met by the host computers. Some examples of cybersecurity deficiencies in the transmitters include a lack of device cyberforensics (no ability to determine what has been changed and by whom), lack of cyberlogging (no ability for long-term storage of information as data are overwritten), no capability of implementing antivirus applications, a lack of patching capabilities, and the use of insecure communication protocols such as File Transfer Protocol, Modbus, and Bluetooth. This means that compensating controls are necessary and that alternate standards/recommendations are needed to address legacy devices expected to be in use for the next 10–15 years or possibly longer.

NETWORK MONITORING GAPS

The current approach for control system security is to monitor the network for malware or other network anomalies. The network monitoring systems monitor data packets, and network anomaly detection assumes that the process sensors provide correct information (accurate), is authenticated (sensor signals comes from the sensor), and is uncompromised (cybersecure). Yet process sensors have minimal, if any, cybersecurity or authentication.

Moreover, raw sensor signals are not monitored for reliability, safety, or security considerations, which is a major gap.

Network monitoring and threat detection were not sufficient to detect the 2017 Triconex cyberattack in Saudi Arabia. Luck and some mistakes kept the petrochemical plant from a dangerous explosion. The mistakes included the attackers inadvertently tripping the plant twice—in June and then again in August. (A plant is said to "trip" when it ceases production for a reason related to safety.) Without the plant trips, it is questionable whether the malware would have been detected before it could be used to damage the plant.

The focus on the analysis of the Triconex cyberattack, including those by U.S. national laboratories, was on the malware found in the safety systems during the August 2017 outage. However, the plant initially tripped in June 2017, two months before the August 2017 outage when the malware

was discovered. The June plant trip was caused by one emergency shutdown controller. The plant distributed control system (DCS) did not reflect unsafe conditions (the DCS does not monitor cyberthreats).

The culture gap between the networking organizations (whether IT or OT) and plant engineering is common and being reinforced by the continued discussions of IT/OT convergence. That is because the plant engineers and vendor staff who analyzed the controller and responded to the HMI alarms are not OT but engineering/operations—and there is a big difference.

The Stuxnet and Triconex attacks compromised Windows HMIs and engineering workstations. With Stuxnet, the centrifuges were being mechanically damaged for months with no apparent indication of anything but mechanical, systemic design problems. The culture gap between the engineers and the cybersecurity organizations enabled the damage to continue for months until Stuxnet was discovered. In Ralph Langner's treatise, "To Kill a Centrifuge,"[3] Langner was asked if Stuxnet can be used as a blueprint for copycat attacks. The Triton attack appeared to follow the Stuxnet blueprint. The Triconex attack also demonstrated that hacking control/safety systems and controllers was not a Siemens-unique problem but an attack mechanism against control/safety systems regardless of vendor.

> A major shortcoming in most industries is that there is an inability to correlate malware to physical impacts.

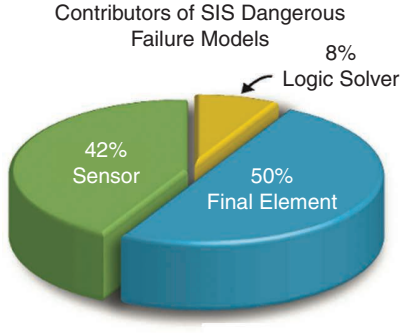

FIGURE 4. The process sensor contribution to safety-integrated systems' (SIS) failure modes. (Source: Offshore Reliability Database.)

Both Stuxnet and Triconex demonstrated the need for an out-of-band monitoring solution that would not be jeopardized by compromising Windows and IP networks.

The serial-to-Ethernet convertors can, and have been, compromised. In the 2015 Ukrainian cyberattack,[4] Internet access allowed access to these unprotected field devices.

A major shortcoming in most industries is that there is an inability to correlate malware to physical impacts (that is, detecting differences between process readings and the conditions the network is reporting or believes to be true). There is a need to be able to observe the process behavior, cross correlate it to the network anomaly, and determine whether there is malware and that the process is changing. Assuming the process is working as expected in real time, there is no need to make changes despite what is coming from the HMI, as opposed to today when there is no real-time, unmodified view of the process.

There is, therefore, a flaw in the network monitoring confidence levels, which will not allow a true, risk-based assessment to be made if malware is discovered on the network when there might not actually be any issue with the process. Higher confidence levels will be achieved when the process can be correlated to the network anomaly.

According to the Offshore Reliability Database, "42% of safety-integrated systems' dangerous failure modes come from process sensors (see Figure 4). 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" that is meant to provide diagnostics that can induce additional cybersecurity vulnerabilities.

An example of adding smartness without a clear understanding of security is a recent hack in Germany. In this case, three-quarters of the building automation systems' (BASs') devices in the office building system's network had been mysteriously purged of their "smarts" and locked down with the system's own digital security key, which was now under the attacker's control. The firm had to revert to manually flipping on and off the central circuit breakers to power on the lights in the building.[5] As mentioned earlier, many of the professionals who install and manage control systems are not on IT or security teams. Rather, BAS systems and level-0,1 devices are typically the domain of engineers and building management firms. IT and cybersecurity teams rarely intersect with BAS operations or level-0,1 engineers and technicians, and that has proven to be problematic.

There are many concerns with a network-only monitoring approach, including the following:

- The SolarWinds hack demonstrated that a sophisticated nation-state attack could compromise even the latest network cybersecurity technologies.
- Ransomware attacks, although aimed at IT networks, can either "leak" into OT networks or cause shutdowns of facility processes due to an abundance of caution.
- There are many control system devices that have no cybersecurity, authentication, or cyberforensics, yet are inputs to IT and OT networks.

- The serial-to-Ethernet convertors that convert the process sensors' analog signals to Ethernet packets for use in an IP network are a "two-way street" into the sensors as well as the networks. The serial-to-Ethernet convertors are often directly connected to the Internet and were compromised as a part of the 2015 Ukrainian power grid cyberattack. Connecting serial-to-Ethernet convertors to the Internet is occurring despite a warning from the U.S. Cybersecurity and Infrastructure Security Agency, issued in May 2015.[6]
- Changing process sensor configurations can affect reliability (prevent restart) or safety (remove equipment protection) with minimal network forensics.
- The network monitoring systems monitor data packets, and network anomaly detection has no other option but to assume that the sensor provides the correct information (accurate), is authenticated (the sensor signal comes from the sensor), and uncompromised (cybersecure). Yet process sensors have minimal, if any, cybersecurity or authentication. However, the Ethernet sensor packet is assumed to be a gold standard, and OT network monitoring techniques are used to ensure that the packet is not compromised. OT network monitoring also assumes that anomaly detection correlates to actual process system impacts.
- OT network monitoring also assumes anomaly detection correlates to actual process system impacts. However, there are no means to correlate network anomalies with physical processes or individual pieces of equipment. That is, if there is malware, what does it mean to a specific pump, valve, motor, relay, and so on? Also, what does it mean to the process?

In other words, what actions should be taken if malware is detected? A network-based approach cannot provide this critical information. Consequently, there is a gap in the network monitoring confidence levels, which will not allow for a true, risk-based assessment to be made when there is a discovery of malware on the network and there might not actually be an issue with the process.

PARADIGM CHANGE

Process sensors, valves, and motors have smart electronics and send serial data (4–20 mA) to the serial-to-Ethernet converters, where data packets are produced and sent onward through the IP network. The raw signal and its higher frequency components (see Figure 5) are filtered out by the gateways. The raw signals are subjected to signal conditioning such as amplification and filtering. Higher frequency components indicative of offset, sensitivity errors, and nonlinearities are filtered out. Therefore, process noise (raw signal) indicative of process and sensor performance (sensor- and process-anomaly detection) are not available for network anomaly detection. Network monitoring starts from the serial-to-Ethernet converters (also known as *serial gateways*) where Ethernet IP data packets are created from analog data from the field devices, with the higher frequency noise filtered out and sent to the HMI.

Every instrument has at least one input and one output. Calibration ensures that the instrument accurately senses the real-world variable it is supposed to measure or control. Ranging establishes the desired relationship between an instrument's input and its output. To calibrate an instrument means to check and adjust (if necessary) its response so that the output accurately corresponds to its input throughout a specified range. To range an instrument means to set the lower and upper range values so that it responds with the desired sensitivity to changes in input. The purpose of calibration is to ensure that the input and output of an instrument reliably correspond to one another throughout the entire range of operation. For many industrial sensors, this graph will be linear. Any linear mathematical function may be expressed in slope-intercept equation form: $y = mx + b$.

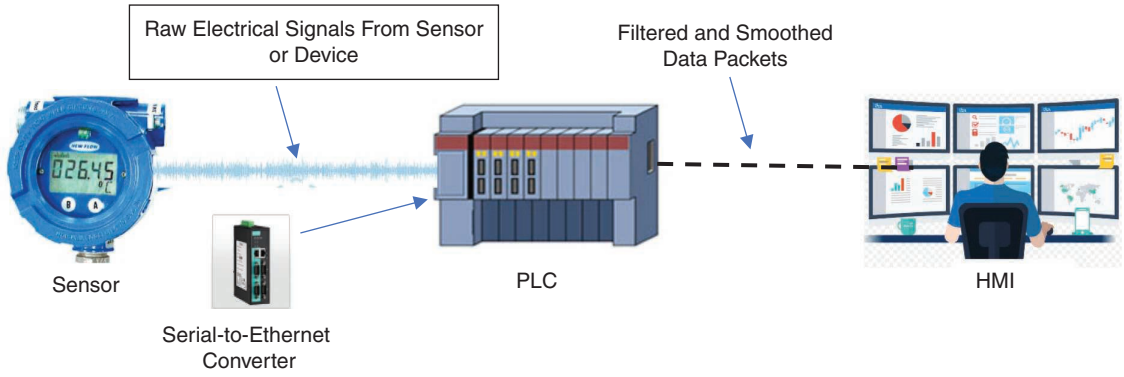

FIGURE 5. The process systems with network anomaly detection.

On the actual instrument, there are two adjustments that match the instrument's behavior to the ideal equation. One adjustment is called the *zero* (or *range*), while the other is called the *span*. These two adjustments correspond to the *b* and *m* terms of the linear function, respectively: the zero adjustment shifts the instrument's function vertically on graph (*b*), while the span adjustment changes the slope of the function on graph (*m*).[7] If the zero or span adjustments are manipulated, this could potentially prevent a sensor from reaching a set point (a safety issue) or reaching a set point before it should (a reliability problem). This type of attack could accomplish what the Triton attack was meant to do, remove the safety function, but would not require modifying any control system logic.

A petrochemical facility was investigating opportunities to increase processing uptime and optimize unit production. As a part of the investigation, the company focused on operator workload and the effectiveness of the existing alarm system. Several areas stood out as opportunities for improvement. Addressing field-related issues, which were typically instrument failure or improper ranging of scale, could reduce nuisance alarms by 50%.[8] The reranged sensors were caused by insiders. Consequently, it was assumed that the failures were unintentional, although they did not have to be. This is a concern as reranged sensors can prevent safety functions. Network anomaly detection would not be able to detect changes to zero and span, whether authorized or not.

OT network monitoring does not have the capability to directly monitor the process because it has no ability to view the process before the Ethernet packet is created. Modern machine learning (ML) algorithms enable pattern detection of the raw process sensor and actuator feedback signals, which 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 cybervulnerabilities. Working together, IT specialists and engineers can pull out their respective toolboxes and identify root causes, which may include cyberrelated causes. In this way, cyberincidents have a much higher probability of detection and appropriate response.

The paradigm change would be to monitor the process sensor electrical characteristics (before the packet is created), which provides a direct view of the health and integrity of the sensors and the process. Real-time process sensor health monitoring needs to start with the raw sensor signal (see Figure 6) before digital filtering occurs. Sensor health monitoring provides a level of trust as electrical characteristics cannot be hacked. An additional benefit of using this approach is that it requires the participation of engineering, which can help solve the culture gap with IT/OT organizations. Monitoring the process sensors in real time (within milliseconds) and cross correlating like (similar) sensors, such as pressure, level, flow, temperature, and motor speed, can minimize false negatives and false positives. Higher network monitoring confidence levels can be achieved when the process can be correlated to the network anomaly. This

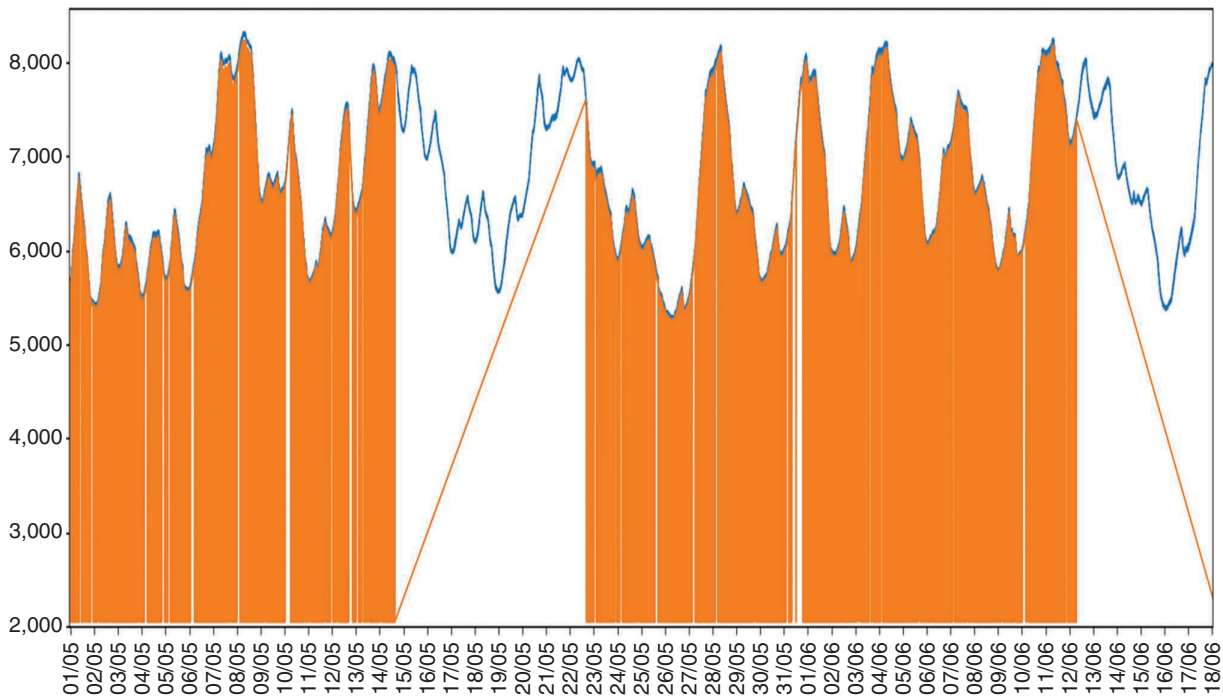

FIGURE 6. Sensor monitoring continues, even with SCADA HMI disruption.

approach can also help with addressing supply-chain and other process issues.

PROCESS SENSOR MONITORING CASE HISTORIES

Process sensors have failed, or been compromised, and the PLCs and HMIs have been unaware. In one case, a process sensor was maliciously hacked, resulting in a turbine being unable to be synchronized to the grid. The serial-to-Ethernet convertors that adapt the process sensor analog signals for use in an IP network are a two-way street into the sensors as well as networks and have been demonstrated to be vulnerable. Changing sensor configurations can affect reliability (prevent restart) or safety (remove equipment protection) with minimal forensics.

The following examples demonstrate that process sensor monitoring can provide an extra level of cybersecurity, safety, and reliability:

- A power utility gas turbine failed to stabilize and deactivated upon fuel feed from both automatic and manual restart. Even after replacing a control card on the main controller, the situation could not be remedied. A costly turbine outage was scheduled. Monitoring the raw sensor data showed a bad temperature sensor (the sensor reading was within the operating range but outside the application range) that was not visible from the HMI. The resulting adjustment allowed for safe turbine activation without a costly outage.
- In chemical plants, bromine reactor anomalies in pH values have a direct impact on production quality and volumes. The sensor monitoring technology quickly identified a previously undetected anomaly at the source, showing that a critical process exceeded the norm, changing pH values and decreasing production. Early identification of the pH process failure enabled immediate correction, saving raw materials and vital process time, and allowed for clarification of work procedures and reporting. The February 2021 Oldsmar water hack of the HMI in Florida[9] was meant to increase sodium hydroxide concentrations to unsafe levels. Monitoring the raw sodium hydroxide (pH) readings would have given a ground-truth measurement of the sodium hydroxide concentrations.
- Existing predictive maintenance was not adequate to address reservoir pump status and process health. The technology monitors more granular data than supervisory control and data acquisition (SCADA). Also, the technology is independent of the SCADA HMI, providing an additional measurement of control and resilience (see Figure 6). Because of the additional granularity, the technology identified an impending pump fault and provided additional system resilience. The sensor monitoring continued to operate even when the OT network was not available. This means that an isolated offline sensor monitoring system would not be susceptible to ransomware or other IT malware. As a result, the Israel Water Authority took the engineering approach and approved offline, out-of-band process sensor monitoring technology to secure the country's water systems. Unlike the prevalent U.S. practice of monitoring IT and OT networks for cybersecurity (that is, for network anomaly detection), the Israeli approach is based on monitoring the electrical characteristics of the process sensors (process-anomaly detection).
- In 2005, the Taum Salk earthen dam in Missouri[10] failed, in part because of a failure in level sensing (see Figure 7). The attachments to the level sensors broke, resulting in the level sensors becoming detached from the wall and providing erroneous low-level information to the SCADA system. As a result of the low-level indication, the SCADA system-initiated pump operation until the upper reservoir overfilled and the dam collapsed. A prototype demonstration with a small plastic tank filled with water and a sensor embedded in the lid of the tank connected to a PLC was used to demonstrate the Taum Salk problem and a possible solution. When the lid of the tank was lifted, the actual level was obviously unchanged. However, the electrical characteristics of the sensor that was embedded in the lid changed. This change in electric characteristics of the sensor could have provided warning of a change in sensor behavior that could have been investigated prior to the dam failure.

> Monitoring the electrical characteristics of process sensors (for example, pressure, level, flow, temperature, voltage, and current) provides a direct view of the process.

APPROACH

One general solution holds great promise because it has the potential

to provide additional cybersecurity, reliability, and safer outcomes for both control and safety systems. Control system situational awareness is dependent on the validity of the process measurement sensors. If the measurements are either inaccurate or compromised, situational awareness is suspect. Monitoring the electrical characteristics of the level-0,1 devices could detect sensor anomalies, whether unintentional or malicious.[11] Specifically, such technology could provide signal authentication. This can address the concerns identified in transformer hardware backdoors, which include communication and spoofing capabilities. The validity and implicit authentication of these devices would be strengthened by monitoring their electrical signal characteristics over time.

Monitoring the electrical characteristics of process sensors (for example, pressure, level, flow, temperature, voltage, and current) provides a direct view of the process. These characteristics would allow for interpretation of any sensor changes whether from sensor drift, process changes, coils heating, unusual equipment vibration, sensing lines clogging, and, importantly, cyber-induced changes. As the electrical properties are physics, they cannot be hacked.

A risk assessment of process sensor cybervulnerability is required for each process plant. It is envisaged that safety analyses such as hazard operational analyses (HAZOPs), control HAZOP/computer HAZOP, layer-of-protection analysis, failure modes and effect analysis, and other reliability and safety studies as well as cyber-specific studies can be drawn upon to identify the critical field devices for which sensor health technology should be installed.

There is also potential for the application of process-anomaly alert systems based on monitoring the raw sensor signals to all industries. There is an opportunity to enhance productivity and reliability in industrial processes through alerting teams to changes in equipment signals and performance while at the same time monitoring for potential cyberthreats.

Monitoring process sensors applies to multiple industries meeting the intent of the U.S. President's Industrial Control System (ICS) Cybersecurity Initiative 14028.[12] 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. Another example is the mining and resource industries. The sensor monitoring system can be applied to any process, machinery, or infrastructure controlled using ICSs, including mineral processing mills, smelters/refineries, power generation facilities, robotic systems and autonomous vehicles, mine hoists, ventilation, telecommunications, water treatment facilities, and associated geotechnical structures such as tailings dams (note how common these process and facilities are to all other industries).

The physical implementation is relatively straightforward. Documentation for the process or as-installed equipment needs to be current, which should be done for any application. Once the 10–15% of critical inputs and outputs are selected, the sensor monitoring system can be engineered based on the incoming signal format, built and shipped to the installation site. Either individual control loops can be taken offline one at a time to allow the system to be connected in parallel to the existing input/output, or the system can be installed during a major ICS shutdown. Once connected and operational, the system goes through a learning period during which models are developed for subsequent downloading into the industrial computer physically located in the sensor monitoring system box. The sensor monitoring system then

> Monitoring for sensor drift can be used to improve the accuracy of digital twins, which inherently assume that sensors are correct.

Taum Sauk Water Storage Dam Failure

Event: In December 2005, the dam suffered a catastrophic failure.

Impact: A billion of gallons of water was released 100 mi south of St. Louis, Missouri.

Specifics: Malfunction in gauges affected automated monitoring system.

Recovery Time:
- replacement dam scheduled for completion in Fall 2009.

Lessons Learned:
- calibrate instrumentation regularly
- add fail-safe redundancy to critical safety systems
- update contingency plans.

Homeland Security

FIGURE 7. The Taum Salk dam failure.[10]

communicates out of band (not through OT/IT networks) using a dedicated wireless modem with a fixed IP address that allows for user interaction, including data downloading through a dedicated web browser. This out-of-band approach prevents the system from being impacted by ransomware or other IT malware—a major benefit.

BENEFITS

Responding to process-anomaly alerts requires teams that do not normally have deep interactions to work together. For example, an alert could be triggered by a change in the process, a sensor calibration drifting, an error in the control system, or a cyberintrusion. Process, operations, maintenance, OT/IT, and risk teams will then be required to work together to determine the root cause and the appropriate response. Breaking down siloed ways of working can be tricky, so JDS Energy and Mining has developed wraparound change management and deployment services to ease the transition.

Because the sensor monitoring system samples the process or machine variables at a higher frequency than most ICSs, the data extracted can also be used to improve troubleshooting and as a data stream source for other advanced process control and ML and/or artificial intelligence applications. The benefits of the sensor monitoring approach include the following:

- Raw process sensor signals provide ground truth about the physical operation of the system. This assumes the use of 4–20-mA 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 unintentional IT or OT 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 semiautomatic 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 that even sophisticated attacks that look like equipment malfunctions will be identified (for example, Stuxnet).
- By monitoring in real time, the system is essentially a sensor-health-monitoring system and also functions as a predictive maintenance system that can be used to extend maintenance intervals for sensors and transmitters.
- 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 cyberincidents.
- 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.
- The 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, and so forth), but real knowledge comes from how the measurements relate to the process or system, and this knowledge resides in the engineers, not the IT specialists.

Monitoring process sensors turns an intractable network security problem into a tractable engineering approach that addresses reliability, availability, productivity, safety, resilience, and cybersecurity while circumventing the cultural issues between network and engineering.

REFERENCES

1. *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*, ANSI/ISA 99-99.00.01-2007.
2. *Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components*, ISA 62443-4-2, Aug. 2018.
3. R. Langner, "To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve," Langner, Nov. 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
4. "Inside the cunning, unprecedented hack of Ukraine's power grid," *WIRED*, 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid
5. "Lights out: Cyberattacks shut down building automation systems," Dark Reading, Dec. 2021. https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems

6. "If you're connected, you're likely infected!" NCCIC/ICS-CERT Monitor, May/Jun. 2015. https://www.cisa.gov/uscert/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf
7. "Instrument zero and span calibration," Instrumentation Tools. https://instrumentationtools.com/instrument-calibration/
8. H. Tanaka, "Control Systems: Optimize alarm management," Chemical Processing, Schaumburg, IL, USA, Nov. 2018. [Online]. Available: https://www.chemicalprocessing.com/articles/2018/optimize-alarm-management/
9. A. Marquardt, E. Levenson, and A. Tal, "Florida water treatment facility hack used a dormant remote access software, Sheriff says," CNN, 2021. https://www.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html
10. "Taum Sauk Dam (Missouri, 2005)," Association of State Dam Safety Officials, Lexington, KY, USA, 2005. [Online]. Available: http://damfailures.org/case-study/taum-sauk-dam-missouri-2005/
11. K. Perumalla, S. Yoginath, and J. Lopez, "Detecting sensors and inferring their relationships at Level-0 in industrial cyber-physical systems," in *Proc. IEEE Int. Symp. Technol. Homeland Security*, pp. 1–5, Nov. 5–6, 2019, doi: 10.1109/HST47167.2019.9032891.
12. "Improving the nation's cybersecurity: NIST's responsibilities under the May 2021 executive order," National Institute of Standards and Technology, Gaithersburg, MD, USA, Presidential Executive Order (EO) 14028, May 12, 2021.

JOSEPH WEISS is a professional engineer and managing partner with Applied Control Systems, LLC, Cupertino, California, 95014, USA. He is an ISA fellow and a Senior Member of IEEE. Contact him at joe.weiss@realtimeacs.com.

ROB STEPHENS is a technology innovator, entrepreneur, and consultant. On industrial control system cybersecurity, he consults with JDS Energy and Mining Inc., Vancouver, British Columbia, V6C 2W2, Canada. Contact him at robstephensphd@gmail.com.

NADINE MILLER is vice president of project development at JDS Energy and Mining Inc., Toronto, Ontario, M5X 1E2, Canada, as well as an independent director of two public mining companies and a strategic advisor to Awz Ventures and Drone Delivery Canada. Contact her at nadinem@jdsmining.ca.

Digital Object Identifier 10.1109/MC.2022.3150947