Control System Cyber Incidents Are Real—and Current Prevention and Mitigation Strategies Are Not Working

Joseph Weiss, Applied Control Solutions, LLC

Rob Stephens and Nadine Miller, JDS Energy and Mining

There is a disconnect between the assumptions and practices within the IT and operational technology communities. This article highlights the disparities in the context of the security and safety of industrial control systems.

Digital Object Identifier 10.1109/MC.2021.3124359
Date of current version: 12 January 2022

The U.S. Presidential Decision Directive (PDD)63[1] states that critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government, including, for instance, telecommunications, energy, banking and finance, transportation, water systems, and emergency services. Within the United States, critical infrastructures have historically been physically and logically separate systems that had little interdependence; they operated as individual islands of automation with minimal to no hardwired interconnectedness. As a result of advances in IT and the necessity of improved efficiency and productivity, these infrastructures have become increasingly automated and interlinked.

Control loops were originally automated using single-loop pneumatic

0018-9162/22©2022IEEE

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

controllers or simple electrical relay circuits. Advances in microelectronics led to the introduction of supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), and distributed control systems (DCSs). Advanced control algorithms have been built on top of these networked systems. Machine learning and artificial intelligence are playing increasingly important roles in the automation of critical infrastructures.

These advances in control system automation introduce vulnerabilities into critical infrastructure systems; these vulnerabilities are associated with equipment failure, human error, weather and other natural causes, and physical and cyber-based attacks. Addressing these vulnerabilities requires flexible, evolutionary approaches that span both control system vendors and end users and protect both domestic and international security. Given the seemingly never-ending parade of serious control system cyber incidents, it is clear the current prevention and mitigation cybersecurity strategies are not working.

DEVELOPMENT OF SILOS

Prior to PDD63 and the attacks of 11 September 2001 (9/11), cybersecurity was simply one of the risks that had to be considered when designing and implementing control systems. Other risks to be considered included seismic, environmental, fire, and reliability risks, among others. Those 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, the engineering organization was responsible for the safe and reliable operation of the equipment, and this included cybersecurity. It was a bottom-up approach of process anomaly detection, performed in the interest of mission assurance. In fact, this was the original basis of the Electric Power Research Institute's control system cybersecurity program started in 2000.[2]

Critical infrastructure cybersecurity practitioners have assumed that Internet Protocol (IP) networks are needed to keep lights on, water flowing, telecommunication links active, and so on. However, for more than 80 years, the grid and other infrastructures operated without an IP network. Control systems in power systems are designed to work in coordination with each other, so the equipment associated with them can work without the SCADA system and its network. As an example, following the 2015 cyberattack on the Ukrainian power grid, the Ukrainians continued to operate the grid manually for months without IP networks because the IP networks could not be trusted. However, the grid—or any other critical infrastructure—could not be operated if the critical control systems or hardware were compromised or damaged.

Sometime after 9/11, cybersecurity for critical infrastructure in the United States became a top national security priority. Around the same time, cybersecurity for control systems was moved to IT—now operational technology (OT)—network monitoring organizations, with domain engineering no longer involved. As a result, control system cybersecurity went from a mission assurance to an information assurance function.

The focus on networks rather than on the process or mechanical or electrical systems can also be seen by having the chief information security officer (CISO) and not the vice president of engineering/operations responsible for the cybersecurity of control systems. Consequently, cybersecurity monitoring and mitigation tended to move to the IP network layer where IT organizations were most comfortable—network anomaly detection tended to replace process anomaly detection, and domain engineering was removed from the design and operating aspects of cybersecurity.

CONTINUING THREATS

A recent article in *Journal of Critical Infrastructure Policy* discusses control system cybersecurity, but it does not focus on a specific critical infrastructure.[3] Another article, which appeared in 2010, provides examples of control system cyber incidents.[4] Examples of serious control system cyber incidents since 2010 include Stuxnet, Havex, BlackEnergy, CrashOverride,[5] and the SolarWinds hack.[6] CrashOverride was the malware that required the Ukrainians to manually operate their power grid. The Triton attack, which targets safety-instrumented systems in particular, is extremely worrying because the intent is to damage equipment and cause mass casualties.[5]

Common threads

There are common threads in what has been missing in addressing control system cybersecurity in all infrastructures:

- common definitions
- the assumption that appropriate network cybersecurity can solve the problem
- the identification of and information sharing about actual incidents
- the lack of cybersecurity of control system devices (for example, process sensors, actuators, and drives)
- the culture gap between networking and engineering.

The productivity benefits of modern networked systems are undeniable. The question is this: at what point and for which applications do the cyber vulnerabilities have a potential greater negative impact compared to positive productivity improvements? This tradeoff assessment has not been adequately addressed.

Moreover, the culture gap between the networking and engineering organizations contributes to an inability to adequately address the tradeoffs. The purpose of this article is to inform discussions about the tradeoffs.

Common definitions

Control systems. Control systems manage, command, direct, or regulate the behavior of other devices, processes, or systems using control loops. They include single-loop controllers; SCADA systems; plant DCSs; PLCs; field devices including process sensors, actuators, and drives; operator displays; process historians; control system networks; and other control system devices. Control systems can range from a single home-heating controller using a thermostat for a home furnace to the large industrial control systems (ICSs) used for controlling processes or machines, from fly-by-wire aircraft to autonomous vehicle control systems.

Cyber incident. A 2021 May Government Accountability Office report[7] defines a *cyber incident* as follows:

> *[A]n event that jeopardizes the cybersecurity of an information system or the information that the system processes, stores, or transmits; or an event that violates security policies, procedures, or acceptable use policies, whether resulting from malicious activity or not. Cyber incidents, including cyberattacks, can damage information technology assets, create losses related to business disruption and theft, release sensitive information, and expose entities to liability from customers, suppliers, employees, and shareholders.*

Note that most control system cyber incidents have not been made public. Consequently, the independent verification of these incidents and an analysis of their root causes are often not possible. Moreover, the focus of the definition is on information—not on the process or system being controlled in the case of control system cybersecurity.

Purdue reference model. The Purdue reference model, shown in Figure 1, provides a model for enterprise control that end users, integrators, and vendors can share in integrating applications at different layers in the enterprise. There are various definitions for the different levels:

- *levels 0 and 1*: the physical process, process sensors and actuators, analog-to-digital conversion, and dedicated controllers for specific functions, such as batch control and variable frequency drives for the speed control of electric motors [timeframe: real time (microseconds) to seconds]

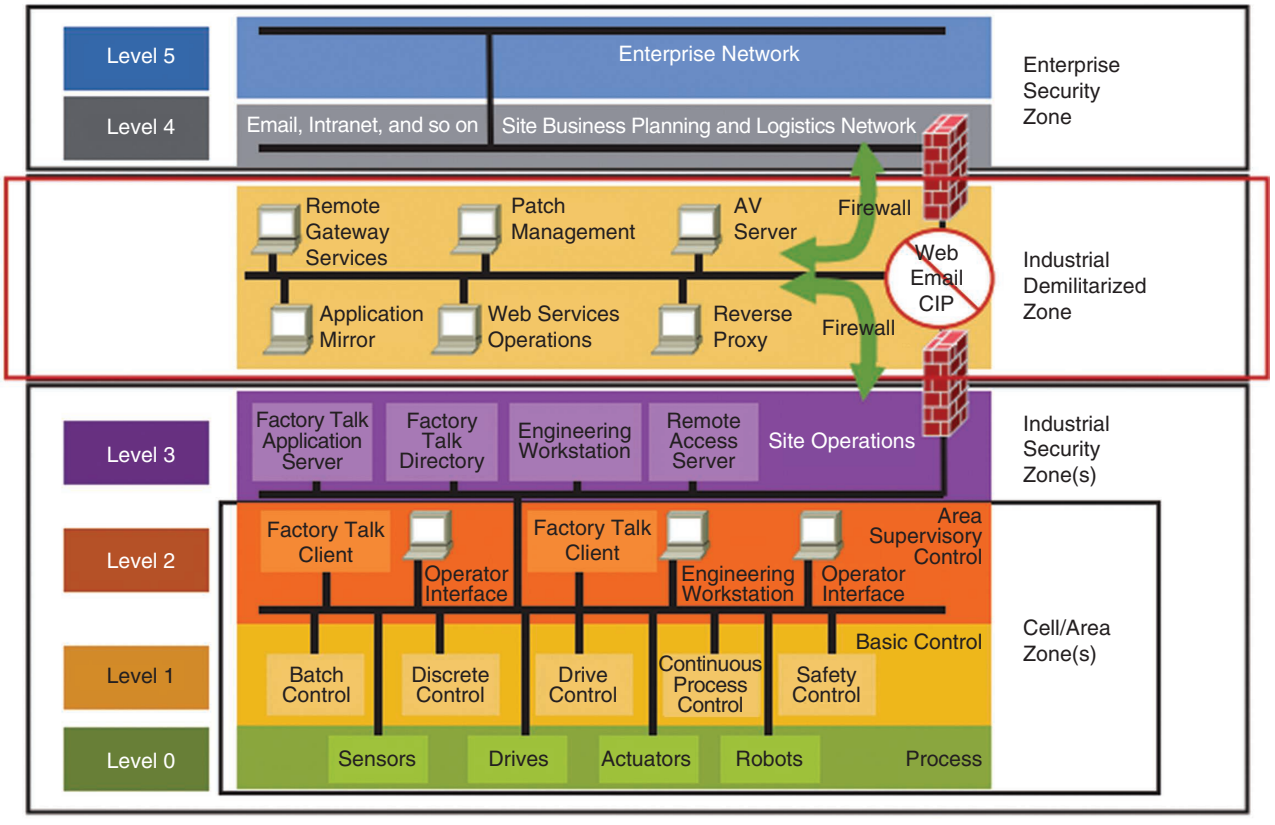

FIGURE 1. The Purdue reference model. (Source: Greenfield.[8]) AV: antivirus; CIP: Critical Infrastructure Protection plan.

- *level 2*: regulatory control, including PLCs, the local plant/facility networks, and human–machine interfaces (HMIs) (timeframe: seconds to minutes)
- *level 3*: supervisory control, encompassing laboratory, maintenance and plant performance management systems, data historians, and related middleware (timeframe: minutes to hours)
- *level 4*: business and enterprise resource planning systems (timeframe: hours to weeks)
- *level 5*: the Internet and cloud.

Note that modern smart wired and wireless transmitters blur the Purdue reference model levels. These modern devices act as a level 0 or 1 sensor, level 2 controller, and—with Ethernet ports—level 3.5 gateway to the business systems, Internet, and cloud.

OT. For the purpose of this article, OT includes control system networks and the personnel responsible for them. Conversely, it does not include equipment such as turbines, valves, or electrical switchgear or the engineers and technicians responsible for the equipment.

Wrong assumptions

The assumption that appropriate network cybersecurity can solve the problem has been challenged by two recent issues—one from Russia and another from China—to the point that relying on network cybersecurity alone should now be recognized as a fatal flaw. The Russian SolarWinds cyberattack[6] demonstrated several key points:

- Sophisticated nation–state attackers can compromise any IP network, regardless of the cyberdefenses employed.
- People issues can defeat even the most sophisticated cybersecurity technologies.
- Even the best cybersecurity organizations can be hacked and not be aware until it is too late.
- Cyberattacks that affect control systems are not always readily identifiable as being cyber related.

The Chinese installed hardware backdoors in large electric power transformers that bypassed all cybersecurity protections and resulted in Emergency Presidential Executive Order 13920.[9] By accessing the hardware back door, a rogue actor could take control of the transformer without accessing it through the IP network.

Attackers wanting to cause damage often use novel approaches that defeat existing monitoring methods. Control systems are systems of systems. Consequently, when one device or system is compromised, it can impact many others, potentially numbered in the tens of thousands.

IDENTIFICATION AND INFORMATION SHARING OF REAL INCIDENTS

Control system cyber incidents continue to occur in industries globally. The impact from these control system cyber incidents ranges from trivial to significant environmental damage, considerable equipment/facility downtime, widespread electric outages, to deaths.

It is not always evident which incidents are malicious. However, it is the impacts that are important. There have been almost 12 million control system cyber incidents in multiple industries globally, resulting in more than 1,500 deaths and more than US$90 billion in direct damages.[10] Regardless of whether the incident is unintentional or malicious, the resulting loss can be the same in its level of severity. In addition, most of these incidents were never identified as being cyber related. Keep in mind that a sophisticated attacker can make a cyberattack look like an equipment malfunction.[11]

There are only a limited number of control system suppliers that provide equipment to control system users worldwide. Around the world, most industries and facilities utilize similar control system devices with the same or similar cyber vulnerabilities. Many of the control system cyber incidents have affected multiple industries. Consequently, there is a large and growing need to share information across all industries.

Why the lack of reporting?

There are minimal to no control system cyberforensics below the IP level and almost no training for engineers to identify whether an upset condition or sensor malfunction could possibly be cyber related. For example, the chemical plant in Saudi Arabia that was the victim of the Triton attack on the safety systems was restarted with malware still in the system, as no one realized that the plant shutdown was caused by malware.[12] It was not until a second shutdown occurred that it was recognized as a cyberattack.[5] The culture gap between engineering and computer networking can exacerbate our inability to detect a control system cyberattack.

Companies and organizations are usually reluctant to publicly acknowledge they have been the victim of a cyberattack. Most cyberattacks on large public companies are evaluated to be below the materiality threshold required for financial reporting. Reporting requirements tend to apply to data breaches, not property damage, injuries, or loss of life. Internet of Things legislation focusing on data breaches will likely make this lack of control system cyber incident reporting even more of a challenge. This can be seen from the recent pipeline cyberattack disclosures from the U.S. Transportation Security Administration (TSA),[13] where the reported cyberattacks did not cause any pipeline damage or equipment shutdowns. Compare that to the previous actual cyber-related pipeline ruptures which would not have been reportable according to the TSA cyberattack reporting requirements.

There are minimal control system cyberforensics and logging for control system field devices as well as minimal training for operational personnel to identify control system cyber incidents. This contributes to

there being few of them that are publicly identified.

There are common threads to many of the ICS cyber incidents beyond the traditional IT breakdowns given in the ICS Computer Emergency Response Team (CERT) report.[14] In the 2007–2010 timeframe, Applied Control Solutions was under contract to MITRE supporting the National Institute of Standards and Technology (NIST) to extend NIST 800-53 for control systems. As part of that effort, three real public cases were used to demonstrate how the extended NIST 800-53 standard would be useful to nonfederal government organizations:

- the Maroochy Shire wastewater SCADA attack[15]
- the Olympic Pipeline rupture[16]
- the Brown Ferry 3 nuclear plant broadcast storm.[17]

All of these cases are also addressed in detail elsewhere.[4] The Olympic Pipeline incident (in Bellingham, Washington) was very similar to the 2010 Pacific Gas & Electric (PG&E) San Bruno (in California) natural gas pipeline rupture in many ways, despite occurring 10 years earlier; this implies that the lessons are not being learned and implemented as well as that silos still exist between infrastructure operators—natural gas versus gasoline. Both involved SCADA maloperation, killed people, and contributed to the bankruptcies of these companies, and neither would have been identified by the recent TSA pipeline cybersecurity guidelines.

From a control system (cyber) perspective, Table 1 outlines the commonalities between the Olympic Pipeline gasoline pipeline rupture and the PG&E natural gas pipeline ruptures. The delayed leak detection response in the 2021 Southern California crude oil pipeline rupture may also be due to similar causes.[18]

Consequently, there is a need to connect the dots and provide guidance to industry. As these cases were not viewed as malicious cyberattacks, they have been largely ignored by the cybersecurity community, even with the latest TSA requirements for reporting on pipeline cybersecurity incidents.

There is a need to use the knowledge from previous control system cyber incidents when developing cyberforensics and monitoring technologies, cybersecurity technologies, and training as well as to adjust requirements such as the North American Electric Reliability Corporation Critical Infrastructure Protection plans, U.S. Nuclear Regulatory Commission Regulatory Guide 5.71/NEI-0809, and Chemical Facility Anti-Terrorism Standards to address what has actually been happening.

Physics-based control system cyber incidents

As mentioned, cyberthreats are generally assumed to occur via IP networks and the associated malware. Physics-based vulnerabilities, such as Aurora,[19] do not need malware but, rather, use remote access (which makes the event cyber related) to cause equipment to operate in "forbidden operating zones" where physics causes actual physical damage.

The Aurora vulnerability occurs when electric substation breakers are opened and then reclosed out of phase with the grid. The out-of-phase

TABLE 1. A comparison between the Olympic and PG&E San Bruno Pipeline failures.

Olympic Pipeline (gasoline)	PG&E San Bruno Pipeline (natural gas)
There were known previous SCADA problems.	There were known previous SCADA problems.
SCADA and leak detection were on the Ethernet LAN.	SCADA (not sure about leak detection) was on the Ethernet LAN.
Previous construction (a water line) impacted the structural integrity of the pipeline months prior to the accident.	Previous construction (a water line) impacted the structural integrity of the pipeline months prior to the accident.
There was no SCADA cybersecurity training.	There was no SCADA cybersecurity training.
There were numerous NIST SP800-53 control violations.	There were numerous NIST SP800-53 control violations.
On the day of the incident, the SCADA system became inoperable (going from a 3–7-s scan rate to being totally inoperable immediately prior to the pipeline failure) and was unable to remotely monitor or actuate the control valves. There were anomalies with sensing.	Just before the incident, PG&E was working on its uninterruptable power supply, resulting in a reduction in the power supply to the SCADA system. Because of this anomaly, the electronic signal to the regulating valve for line 132 (to San Bruno) was lost. The loss of the electrical signal resulted in the regulating valve moving from the partially to fully open position, as designed. There were anomalies with sensing.
Operator displays did not indicate a loss of SCADA functionality.	Operator displays did not indicate a loss of SCADA functionality.
The leak detection system did not function in a timely manner.	The leak detection system did not function in a timely manner.

LAN: local area network.

condition generates large torques and current spikes that can damage the ac equipment and transformers connected to those breakers.[20] The Aurora demonstration proved there could be physical damage from an attack, though the operators were blind because the attack was not seen from the SCADA system.

As Aurora can damage critical equipment with a long lead time for construction and delivery, this type of attack can result in long-term outages. For example, the lead time for replacements for grid-scale high-voltage equipment and/or turbogenerators is on the order of more than eight to 10 months or longer rather than hours, days, or even weeks, as envisaged by most before the Aurora demonstration.

CONTROL SYSTEM FIELD DEVICES (LEVELS 0 AND 1)

Process sensors measure the pressure, level, flow, temperature, voltage current, motor speed frequency, chemical composition, and so on. These devices are ubiquitous. A process facility may have 10–100,000 of them, a large ship could have 50–100,000, a utility-scale solar facility can have millions, and commercial office buildings might have thousands.

Process sensor monitoring has been used for many years for process anomaly detection. Process sensors can generate anomalies for a number of reasons. The process sensing line could be fouled, the sensor output might have drifted, the process or system characteristics could have changed, and/or the sensor input or the analog-to-digital conversion process could have been compromised. In some cases, the sensor output needs to be sampled at a sufficiently high frequency, generally greater than that at which most control systems operate, to understand the changed sensor output characteristics.

Control system devices, such as protective relays, work on instructions entered into registers within their hardware. 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 measurement and register instructions. The instructions sent to the protective relay in the Aurora demonstration that destroyed the generator set involved no malware, unlike what was stated in Andy Greenberg's *Wired* article.[21]

Level 0 or 1 devices often are the least understood part of control system cybersecurity, yet they can have some of the most significant impacts. As an example, on 30 March 2021, Dr. Juan Lopez from the Oak Ridge National Laboratory and the lead author gave a workshop, "Changing the Paradigm of Control Systems Cybersecurity," at the 76th Texas A&M Instrumentation and Automation Symposium. The participants in this conference were some of the leading control, safety, and human interaction experts, yet the lack of cybersecurity for process sensors was new to many of them.

Legacy engineering field devices such as process sensors, actuators, drives, positioners, and analyzers have no cybersecurity, authentication, or cyberlogging, nor can they be easily upgraded for cybersecurity. However, process sensor data are the input to process control, safety systems, OT networks, predictive maintenance programs, historians, and so on, where the sensor input is assumed to be uncompromised, authenticated, and correct. However, because the sensor input is not authenticated, it is not clear that the apparent sensor data are actually coming from the sensors and not from "spoofed" signals. The actuators, drives, controllers, and so on receiving the sensor signals have no way to authenticate their origin and, therefore, automatically accept the sensor output and respond accordingly.

Those assumptions, at the very least, depart from the IT principle of "zero trust." Compromising process sensors (or not recognizing sensor deviations) can circumvent cybersecurity mitigation as well as engineering safeguard protections. However, there is minimal cybersecurity in the process sensor ecosystem. Worse, there are built-in vulnerabilities that cannot be bypassed.

These are not idle considerations. Process sensor issues have been directly involved in many control system cyber incidents. Russia, China, Iran, and other state actors are aware of the cybersecurity gaps in these devices—in many cases, their own critical infrastructures use the same control systems as the rest of the world. The spoofing of transformer sensor signals could be the approach the Chinese are using with hardware backdoors in a large electric transformer to take control of it without needing to hack the networks and risk an unexpected shutdown or similar identifying event as occurred when Russia tried to unsuccessfully hack the safety systems in the Triton attack.[5] Therefore, there is a need to take an intractable network monitoring approach and make it a tractable engineering program.

Modern machine learning enables the pattern detection of raw process sensor signals, which was not previously possible. It is this additional capability that enables sensor monitoring to identify process anomalies regardless of the cause and independent of IP networks and their associated cyber vulnerabilities.

As a result, the Israel Water Authority recently took that engineering approach, approving offline process sensor monitoring technology to secure the country's water systems.[22] Unlike the prevalent U.S. practice of monitoring IT and OT networks for cybersecurity (that is, for network anomaly detection), the Israeli method is based on monitoring the electrical characteristics of the process sensors (process anomaly detection) and not just relying on network monitoring. This approach should be seen as complementary but required in addition to network anomaly detection to have a complete system.

Level 0 or 1 devices are often at the root of technical and organizational

issues, as they are directly used in safety, control, maintenance, and operations, often with different requirements, users, and organizational cultures. The organizational problem at levels 0 and 1 is very complex. Furthermore, the organizational issues may be different on the user versus the vendor side. They manage different problem spaces and have different goals and strategies. Moreover, there have been no Industrial Control System Cyber Emergency Response Team level 0 or 1 device cybersecurity vulnerability disclosures nor any cybersecure certifications for process sensors, actuators, and so on.

GAPS IN STANDARDS

The available standards mostly reflect the divisions in end-user organizations. For instance, the International Society of Automation (ISA) 99[23] cybersecurity standards exclude safety, while ISA 84[24] safety standards have not addressed the unique issues of cybersecurity (which are now changing). Additionally, many device safety manuals do not mention cybersecurity, and, conversely, many cybersecurity manuals do not mention safety. The ISASecure certification program[25] Component Security Assurance focuses on the cybersecurity of software applications, host devices, and network devices.[26] To date, there have been no process sensors certified to ISASecure because of the example technical gaps listed next. Moreover, there currently are no cyber requirements for process measurement integrity in the ISA 62443 or IEEE standards.

The ISA 84.09 working group (the process safety/cybersecurity group specifically organized to address safety and security as part of an integrated safety lifecycle) performed a thorough review of a generic state-of-the-art digital safety (wired) pressure transmitter for conformance to the ISA 62443-4-2 standard, *Technical Security Requirements for IACS* [International Annealed Copper Standard] *Components*.[27] Pressure transmitters were selected, as they are used in both basic process control and process safety applications. Other transmitter types such as differential pressure, temperature, level, and flow as well as other process transmitters will likely have similar cybersecurity issues. Many of the review conclusions are also applicable to wireless and analog sensors, though they were not explicitly addressed in this assessment.

There is a prevailing thought that analog sensors cannot be hacked because they are accessible only from close proximity to the sensors. That is not true and has been demonstrated by various security researchers, including those from Russia using a project called *Corsair* in 2014.[28] There were other similar demonstrations and papers, such as one from Dr. Juan Lopez, then at the U.S. Air Force Institute of Technology.[29] These existing wired and wireless digital and analog pressure transmitters with their cybersecurity limitations are expected to continue to be produced and used for at least the next 10–15 years, so "rip and replace" is not a solution.

The intent of the ISA 84.09 effort was to determine the relative conformance and applicability of the ISA 62443-4-2 Component Specification's individual security requirements to the legacy (what is being built today and 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 requirements, could not be met with this state-of-the-art sensor system.

However, some of the requirements could be met by the host computers, such as secure boot. Selected example cybersecurity deficiencies in the transmitters include the following:

- a lack of device cyberforensics (no ability to determine what has been changed and by whom)
- a lack of cyberlogging (no long-term storage of information as data are overwritten)
- no ability to implement antivirus approaches and a lack of patching capabilities
- the use of nonsecure communication protocols such as FTP, Modbus, Bluetooth, and so on.

This means that compensating controls are necessary and that alternate standards and recommendations are needed to address the legacy devices that will be in use for the next 10–15 years or longer. There are compensating controls that can be developed to meet some, but not all, of the pressure transmitter cybersecurity deficiencies. This effort is ongoing within the ISA 84.09 committee. This work includes the continuation of this use case, which is part of a broader case study to illustrate practical activities within the overall integrated safety/security lifecycle. The hope is that discussions with manufacturers will help to improve the transmitter study and begin formalizing potential compensating countermeasures. Additional offshoots expected from this exercise are better guidance for security manuals and their relationship to safety.

GAPS IN GOVERNMENT APPROACHES

On 28 July 2021, an announcement was made about President Biden's ICS Cybersecurity Initiative, 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 cyberthreats. As mentioned, control system field devices, such as pressure, level, flow, temperature, and voltage sensors (often not considered part of OT), are inherently insecure. The President's ICS Cybersecurity Initiative is not addressing this fatal flaw.

THE LIMITS OF NETWORK SECURITY

The disadvantages of the current U.S. approach include the following:

- Neither IT nor OT networks provide ground truth about the

process and assume the sensor input is uncompromised, authenticated, and correct.
- Network monitoring is a never-ending "whack-a-mole" issue. In other words, defenders come up with attack-scenario protection, and then attackers come up with a bypass solution.
- Even supposedly high-quality network cybersecurity can be defeated, as demonstrated by the SolarWinds hack.
- OT networks are susceptible to unsophisticated as well as sophisticated network vulnerabilities.
- OT cybersecurity organizations tend to exclude the engineers responsible for the design and operation of the control systems.

GAPS IN CULTURE AND EDUCATION

The culture gap between IT-based networking and facilities/engineering organizations, shown in Figure 2, continues unabated. The gap begins in universities and colleges. Cybersecurity is taught in computer science, where there is often no requirement for taking an introductory course in engineering focused on processes or mechanical and electrical systems. In parallel, engineering curricula typically do not include an introductory course in cybersecurity or even address it in any depth in process or control system courses. The two teams that need to play well together do not even comprehend what the other one knows, and there is no common language.

The lack of the cybersecurity organizations addressing level 0 and 1 devices is one of the significant reasons for the broken (or never-established) culture gap between IT and OT teams and operations and engineering teams.[30] However, the gap in understanding also affects engineering organizations.

With respect to process sensor cybersecurity, the authors are not alone in our concerns. A respected colleague stated, "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." Additionally, the 19 October 2021 ISA 62443 Conference had a senior government official respond to why they are not addressing securing level 0 and 1 devices: "It's hard."

Currently, almost all cyber policy-making organizations are led by the CISO. However, often, he or she is not an engineer and does not deeply understand the operational needs. As a result, there are few cyber policy-making organizations that include senior representatives from the engineering or facilities organizations. This has resulted in numerous cases where IT network security technology or testing has affected control systems or plant operation. In one case, 6,000 controllers were shut down by IT network scanning.[32] This can also be seen in the lack of addressing OT systems in data center cybersecurity assessments.[34]

The National Society of Professional Engineers (NSPE) recently published an article addressing the aforementioned challenges.[33] Specifically, networking and engineering organizations have different priorities. Engineering is focused on process reliability and safety. This means that it is concerned with whether a cyber incident is malicious or unintentional, whereas the networking organization is focused on network availability and data breaches (malicious attacks). This gap can be observed in the companion blogs.[34,35]

The gap between IT and engineering can also be seen in the cybersecurity standards utilized by each organization. For IT, that is generally the ISO 27000 series of standards. For engineering, it is usually the ISA 62443 series of standards.

Lucian Niemeyer, CEO of the Building Cyber Security Consortium and a former U.S. assistant secretary of defense, stated, in his presentation on 6 October 2021 at the Industrial Internet of Things World's Cybersecurity Day,[36] that approximately 10% of an IT budget should be spent on security. However, because engineering organizations are generally not participating in cybersecurity discussions, the metric is for the IT budget. Therefore, the security budget will not necessarily be adequately appropriated for the engineering organization at vendor or end-user organizations. This contributes to the culture gap and, in turn, lack of cybersecurity in control system products. Until the culture gap can be overcome, there is little

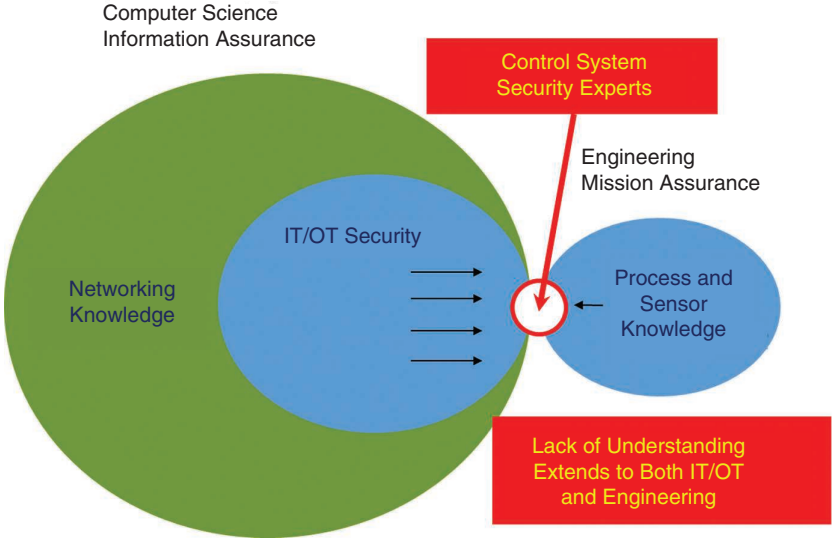

FIGURE 2. The culture gap between networking and engineering. (Source: Weiss.[31])

chance of adequately cybersecuring any critical infrastructures.

Control system cybersecurity incidents continue to occur despite significant efforts to prevent them. People die or are injured; significant environmental damage occurs; process plants and other systems are compromised, sometimes to the point of equipment destruction; and companies and organizations sometimes fail as a result of control system cybersecurity incidents. However, these occurrences, some of which are high in the severity of the outcome, are generally not identified as being cyber related, as there are often minimal cyberforensics for them and no cybersecurity training for the control system engineers and other engineering and operations staff to even ask the question of whether it could have been a cyber incident.

The current approach to control system cybersecurity is driven by IT/OT teams that are comfortable in the world of network security and information protection. However, their focus ignores the fatal flaw posed by the lack of cybersecurity for the level 0 and 1 sensors, transmitters, controllers, and actuators. IT/OT as well as engineering/operations organizations, in many cases, do not even recognize that the issue exists.

This commentary is intended to raise awareness of the critical fatal flaw of assuming device level 0 and 1 integrity without any checks. In a follow-up article in this column, the authors will provide recommendations to address the issue.

REFERENCES

1. "Critical infrastructure protection," Presidential Decision Directive (PDD), May 22, 1998. [Online]. Available: https://irp.fas.org/offdocs/pdd/pdd-63.htm
2. "Cyber security primer," Electric Power Research Institute, Palo Alto, CA, USA, Rep. TR100797, Sept. 2000.
3. J. Weiss, "Control system cyber security," *J. Crit. Infrastructure Policy*, vol. 1, no. 2, pp. 111–135, Nov. 2020, doi: 10.18278/jcip.1.2.7.
4. J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*. New York, NY, USA: Momentum Press, May 2010.
5. M. Giles, "Triton is the world's most murderous malware, and it's spreading," *MIT Technology Review*, Mar. 5, 2019. [Online]. Available: https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/
6. S. Oladimeji and S. M. Kerner, "SolarWinds hack explained: Everything you need to know," TechTarget, Jun. 16, 2021. [Online]. Available: https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know
7. "Cyber insurance insurers and policyholders face challenges in an evolving market," Government Accountability Office (GAO), Washington, DC, GAO Rep. Accessed: May 2, 2021. [Online]. Available: https://www.gao.gov/assets/gao-21-477.pdf
8. D. Greenfield, "Is the Purdue model still relevant," AutomationWorld, May 12, 2020. [Online]. Available: https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant
9. " Securing the United States bulk-power system," Federal Register, May 1, 2020. [Online]. Available: https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system
10. "Control system cyber incidents are much more plentiful than people realize," Control. Accessed: May 2, 2021. [Online]. Available: https://www.controlglobal.com/blogs/unfettered/control-system-cyber-incidents-are-much-more-plentiful-than-people-realize
11. J. Fruhlinger, "What is Stuxnet, who created it and how does it work," CSO Online, Aug. 22, 2017. [Online]. Available: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html
12. "Control system cyber attacks have become more stealthy and dangerous—and less detectable," Control, Jul. 4, 2019. [Online]. Available: https://www.controlglobal.com/blogs/unfettered/control-system-cyber-attacks-have-become-more-stealthy-and-dangerous-and-less-detectable/
13. "TSA cyber security requirements are still not addressing control system-unique issues," Control, May 27, 2021. [Online]. Available: https://www.controlglobal.com/blogs/unfettered/tsa-cyber-security-requirements-are-still-not-addressing-control-system-unique-issues
14. "ACTUAL domestic and international ICS cyber incidents from common causes," Control, Aug. 2, 2015. [Online]. Available: https://www.controlglobal.com/blogs/unfettered/actual-domestic-and-international-ics-cyber-incidents-from-common-causes
15. M. D. Abrams and J. Weiss, "Malicious control system cyber security attack case study: Maroochy shire water services, Australia," Aug. 2008. [Online]. Available: https://www.mitre.org/publications/technical-papers/malicious-control-system-cyber-security-attack-case-study-maroochy-water-services-australia
16. M. Abrams and J. Weiss, "Bellingham, Washington control system cyber security case study," Sept. 20, 2007. [Online]. Available: https://icscsi.org/library/Documents/Case_Studies/Case%20Study%20-%20NIST%20-%20Olympic%20Pipeline.pdf
17. C. Baylon, R. Brunt, and D. Livingstone, *Cyber Security at Civil Nuclear Facilities—Understanding the Risks*, London, U.K.: Chatham House, Oct. 5, 2015. [Online]. Available: https://www.chathamhouse.org/sites/default/files/field/

field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf
18. M. Brown, "California oil spill response in question after delay in shutting down pipeline," *CTV News*, Oct. 6, 2021. [Online]. Available: https://www.ctvnews.ca/climate-and-environment/california-oil-spill-response-in-question-after-delay-in-shutting-down-pipeline-1.5612754
19. M. Swearingen, S. Brunasso, J, Weiss, and D. Huber, "What you need to know (and don't) about the AURORA vulnerability," *Power*, Sept. 2013. [Online]. Available: https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/
20. "cnn auroara generator test," Yahoo! Search. [Online]. Available: https://video.search.yahoo.com/search/video?fr=mcafee&p=cnn+auroara+generator+test#id=2&vid=dd006b5cfc280fed537e950070a492e0&action=click
21. A. Greenberg, "How 30 lines of code blew up a 27-ton generator—A secret experiment in 2007 proved that hackers could devastate power grid equipment beyond repair with a file no bigger than a GIF," *Wired*, Oct. 20, 2020. [Online]. Available: https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/
22. "Israel Water Authority taps SIGA for cyber protection of the country's water supply," Calcalistech, Jul. 21, 2021. [Online]. Available: https://www.calcalistech.com/ctech/articles/0,7340,L-3913012,00.html
23. *Industrial Automation and Control Systems Security*, ISA99. Accessed: Oct. 5, 2021. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99
24. *Instrumented Systems to Achieve Functional Safety in the Process Industries*, ISA84. Accessed: Oct. 5, 2021. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa84
25. ISASecure. Accessed: Oct. 5, 2021. [Online]. Available: https://www.isasecure.org/en-US/
26. *Certified Components*, IEC 62443-4-2, 2007. Accessed: Aug. 13, 2018. [Online]. Available: https://video.search.yahoo.com/search/video?fr=mcafee&ei=UTF-8&p=cnn+aurora+generator+test&type=E211US0G0#id=3&vid=dd006b5cfc280fed537e950070a492e0&action=click
27. "Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components," ANSI/ISA-62443-4-2-2018. [Online]. Available: https://www.isa.org/products/ansi-isa-62443-4-2-2018-security-for-industrial-au
28. "Highlights from the 2014 ICS Cyber Security Conference," Control, Oct. 27, 2014. [Online]. Available: https://www.controlglobal.com/blogs/unfettered/highlights-from-the-2014-ics-cyber-security-conference/
29. J. Butts, B. Mullins, J. Butts, and J. Lopez, "Design and implementation of industrial control system emulators," in Butts and Shenoi (Eds.), *Critical Infrastructure Protection VII, IFIP AICT 417*. New York, NY, USA: Springer, 2013, pp. 35–46.
30. "Engineering, Operations, and Maintenance often do not view cyber security as their problem," Control, Mar. 28, 2021. [Online]. Available: https://www.controlglobal.com/blogs/unfettered/engineering-operations-and-maintenance-often-do-not-view-cyber-security-as-their-problem
31. J. Weiss, "The need for interdisciplinary programs for cyber security of industrial control systems," in *Proc. WorldComp 2010 Conf.*, Las Vegas, NV, USA.
32. "Are your buildings and cloud cyber secure?" Control, Apr. 29, 2021. [Online]. Available: https://www.controlglobal.com/blogs/unfettered/are-your-buildings-and-cloud-cyber-secure
33. J. Weiss, "Attention policymakers: Cybersecurity is more than an IT issue," *PE Magazine*, May/June 2020. [Online]. Available: https://www.pemagazine-digital.com/pemagazine/may_june_2020/MobilePagedReplica.action?pm=2&folio=Cover#pg1
34. "Network security often does not view control system devices and the process as their problem," Control, Apr. 5, 2021. [Online]. Available: https://www.controlglobal.com/blogs/unfettered/ot-network-security-often-does-not-view-control-system-devices-and-the-process-as-their-problem
35. "Engineering, Operations, and Maintenance often do not view cyber security as their problem," Control, Mar. 28, 2021. [Online]. Available: https://www.controlglobal.com/blogs/unfettered/engineering-operations-and-maintenance-often-do-not-view-cyber-security-as-their-problem
36. IIOT World, *Ask Me Anything with Lucian Niemeyer.* (Oct. 8, 2021). [Online Video]. [Online]. Available: https://www.youtube.com/watch?v=G1emf2ns2_s

JOSEPH WEISS is a professional engineer and managing partner with Applied Control Systems LLC, Cupertino, California, 95014, USA. Contact him at joe.weiss@realtimeacs.com.

ROB STEPHENS is a consultant with JDS Energy and Mining Inc., Vancouver, British Columbia, V6C 2W2, Canada. Contact him at robstephensphd@gmail.com.

NADINE MILLER is the vice president of project development at JDS Energy and Mining Inc., Toronto, Ontario, M5X 1E2, Canada. Contact her at nadinem@jdsmining.ca.