Control System Cyber Security

Joseph Weiss, PE, CISM, CRISC[1]

[1] Managing Partner, Applied Control Solutions, LLC, joe.weiss@realtimeacs.com

Abstract

Cyber security for Information Technology (IT)/Operational Technology (OT) is about the protection of Internet protocol (IP) networks from cyber attacks. Control system cyber security is about protecting physical processes from unintentional incidents and malicious attacks. Technologically, control system cyber security is different than IT cyber security because of the control system devices and their low-level communication protocols. Yet IT and OT cyber security policy has been developed by the network security organization with minimal participation from the engineering organizations that "own" the hardware and control systems.

Control system cyber security is real—there have been more than 1,250 actual incidents identified to date.[1] But there currently is widespread lack of appropriate control system cyber forensics and cyber security training. With the availability of IT cyber security hardware, testing, and training, IT systems continue to be compromised, and control system cyber security is arguably 5-10 years behind IT.

In addition to the need to upgrade control system cyber security at the levels of individual organizations and critical infrastructures, this is a matter of national security import. It was widely reported that a large Chinese-built electric transformer may have contained hardware backdoors, allowing access to transformer equipment control parameters. (Wall Street Journal, 2020). Attack vectors in the control system area resulted in Presidential Executive Order (EO) 13920 in May 2020.[2]

1 This observation is derived from a database on control system incidents or cases compiled since 2000 by Joseph Weiss. See "J. Weiss, *Control Unfettered*, "Databases for actual control system cyber incidents exist—and they are important for many reasons," November 18, 2019.

2 Long-term monitoring activities of foreign security services also contributed to the Department of Homeland Security initiative, "Securing Industrial Control Systems: A Unified Initiative, FY2019-FY2023," Cybersecurity and Infrastructure Security Agency, July 2020. See https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf

doi: 10.18278/jcip.1.2.7

Consequently, this paper advocates a paradigm shift to work around the current lack of a robust capability to secure control system networks. In order to address the limitations in securing control legacy and "next generation" control systems and networks, new approaches for improving control system cyber security and the ability to widely deploy them are needed.

Keywords: Control systems, cyber security, Operational Technology, Presidential Executive Order 13920

Introduction

Control systems monitor and guide the operation of physical assets and processes, such as power systems, refineries, pipelines, water and wastewater, chemical plants, strategic industries, manufacturing, building controls, healthcare installations and other critical infrastructures. (As can be seen from this list, control systems are used in more than just "industrial" applications.) Operational technology (OT)/control systems pertains to hardware and software that detect or cause changes through the direct monitoring and/or control of industrial, manufacturing, and commercial equipment, assets, processes and events. What makes control system cyber security different than IT cyber security are its overriding priorities of protecting life and physical property. This applies at the level of a small industrial or manufacturing plant as well as the control room of a utility providing electricity to multiple states.

From 1970s through the mid-1990s, control systems and their accompanying process sensors and other field devices such actuators, drives, and chemical analyzers were not connected to the outside world. They operated under the purview of engineers who designed, operated, and maintained these systems. The design and operational requirements emphasized performance and safety—not cyber security. Control systems and the "dumb sensors" that monitored equipment generated data only useful to engineers, operations, and maintenance. The advent of microprocessors in the late 1960s and Moore's Law allowed the calculation and conversion capability to take the 0s and 1s of engineering data and to convert them to information usable by multiple parties outside the organization's engineering division. It was the availability of this valuable data that led to demand outside of the engineering operation, and often outside the company. It enabled productivity improvements like "just-in-time" operation through data sharing among multiple organizational components. The Internet and modern networking technologies were vehicles for information dissemination and remote systems management.

From an engineering and control system perspective, cyber security was simply a new set of risks to be addressed in designing and implementing systems,

along with reliability, environmental factors, fire threats, seismic risks, and other concerns. Since these were engineering issues, cyber security of these systems was perceived as an engineering function. The intent was to ensure that the engineering design basis would be met regardless of risks. Consequently, at that time, engineers were the front lines of cyber security defense. The focus was from the bottom up. That is, the emphasis was on whether the process could be impacted by cyber threats, which is process anomaly detection, or in other terms, mission assurance.

Following 9/11, cyber security became a mainstay of national security. Because the IT function was responsible for corporate IT cyber security, the cyber security function for control systems was moved from the engineering organizations to the IT organizations within most entities. It was also in this period that engineering was severed from cyber security protection of their own systems. This pronounced shift resulted from cyber security monitoring and mitigation functions gravitating towards the Internet Protocol (IP) network layer. This included the widespread use of Human-Machine Interfaces (HMIs) with commercial-off-the-shelf operating systems, generally Microsoft Windows. Since Engineering was no longer in the forefront, control system cyber security went from being Mission Assurance to Information Assurance. And because these engineering systems were not included under IT's purview, the Level 0, 1 devices[3] were not incorporated in cyber security considerations. The net result is that most legacy engineering systems have no cyber security, authentication, or cyber logging, nor can they be upgraded. The lower level sensor networks such as Highway Addressable Remote Transducer (HART[4]), Profibus,[5] Fieldbus,[6] etc. also have little or no cyber security. hey present an inviting target for potential threats that are not IP-network focused. The different ways that control system architecture and guidelines are perceived by engineers and cyber security specialists causes further divergence.

Cyber security became an IT issue after the first virus/worm was identified in the late 1980s. The Morris worm of November 2, 1988—usually considered the first computer worm and certainly the first to gain significant mainstream media attention—was distributed via the Internet. It resulted in the first conviction in the U.S. under the 1986 Computer Fraud and Abuse Act. IT cyberattacks have proliferated, leading to worldwide attention, diverse mitigation approaches, and government responses.

IT cybersecurity developed technical guidance starting with ISO/IEC27000, which is part of a growing family of ISO/IEC Information Security Management Systems (ISMS) standards within the information and IT security fields. Standards

3 Level 0 = physical process; Level 1 = controllers and intelligent devices including sensors, analyzers, actuators, instrumentation

4 www.fieldcommgroup.org

5 https://www.profibus.com/

6 http://www.fieldbus.org/

include general methods, management system requirements, techniques and guidelines to address both information security and privacy. Importantly, these standards are IT focused and do not address the unique issues associated with control systems, including reliability and safety. This lack of focus on automation and control systems led to the establishment of ISA99, which has developed the suite of IEC-62443 series Automation and Control System Cyber Security Standards specific to Automation and control systems (Figure 1).

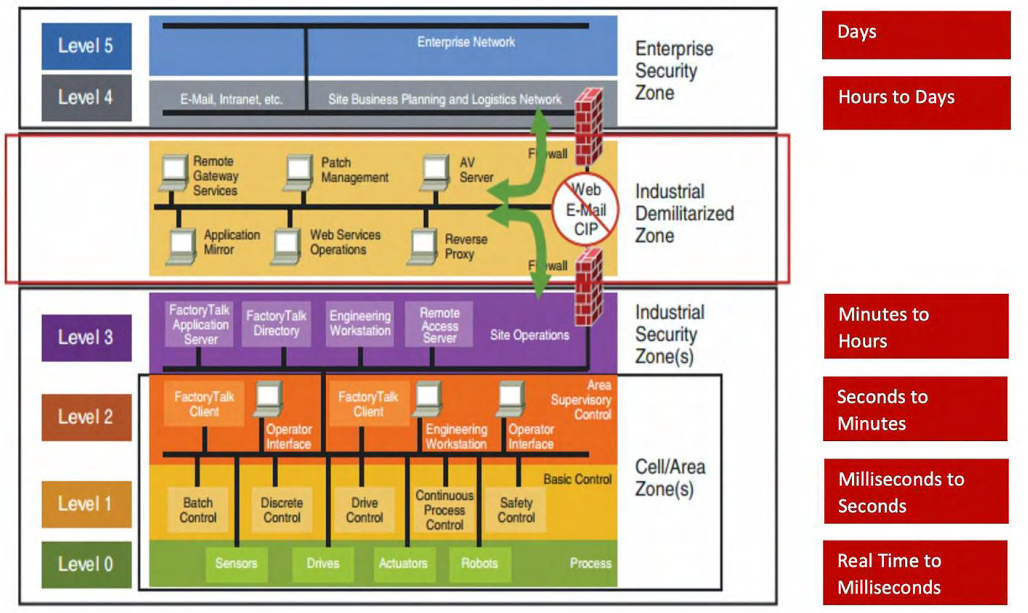

Figure 1. Automation and Control System Cyber Security Standards

Control system information flows do not concentrate on cyber security. The Purdue Reference Model7 (Figure 2) was developed in the 1990s to assure that real-time control system performance was not affected, and secondarily to clarify how information should flow from the plant floor. It was based on existing technology that aligned with the limited capabilities of sensors, controllers, process control networks, etc. With the microprocessor and communication revolutions, the Reference Model levels are no longer so straightforward. These technologies enable process sensors to also have Programmable Logic Controllers (PLC) and even communication gateway capabilities. The Level 0, 1 devices used throughout all physical infrastructures are not cyber secure. In fact, some instrumentation and low-level instrumentation networks may not be able to be secured.

This stands in stark contrast to the International Standards Organization (ISO) seven-layer model that was developed for network communications and security (Shaw, 2018). The ISO Model divides network communication into layers

7 ANSI/ISA99-99.00.01-2007

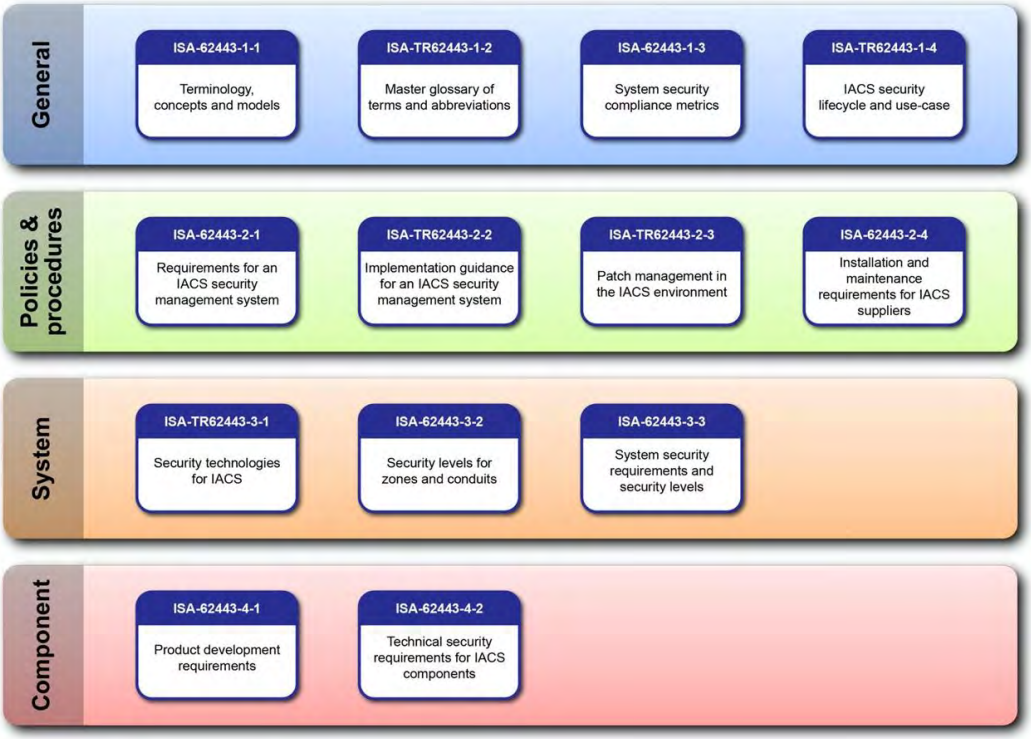

Figure 2. Purdue Reference Model
Source: Rockwell Automation

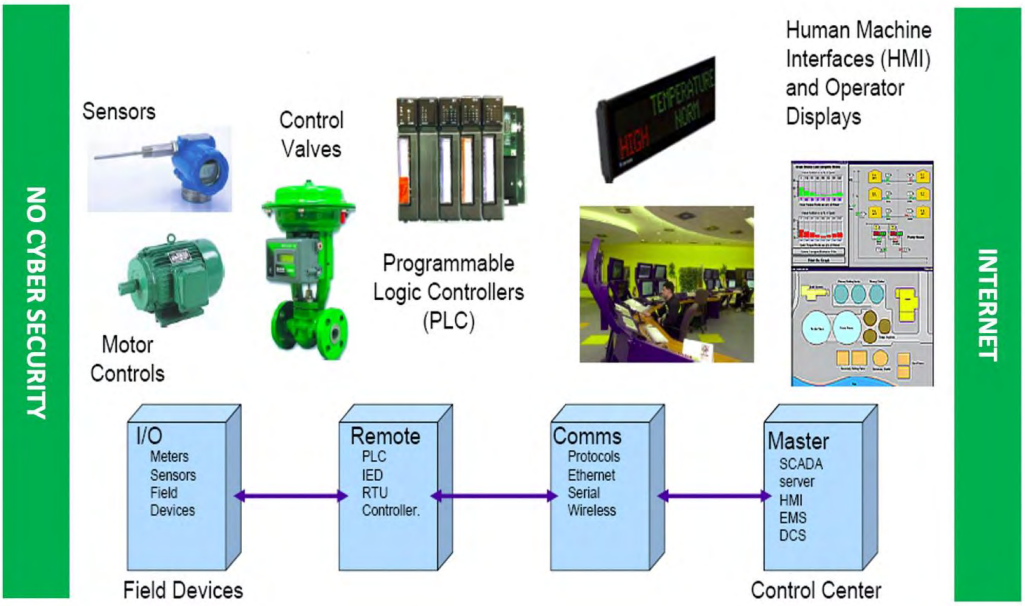

Figure 3. Control System Basics

1-4 which are considered the lower layers, mostly applicable to moving data. They do not consider real time performance or latency in any manner. Layers 5-7, the upper layers, contain application-level data. Networks operate on one basic principle: "pass it on." Each layer takes care of a specific function, and then passes data to the next layer (Shaw, 2018).[8]

A typical control system is composed of Level 0,1 devices (e.g., process sensors, actuators, and drives) connected to Level 2 controllers that are linked to process control networks and Human Machine Interfaces (HMIs), also known as operator displays, at Level 3. In turn, they are connected to archival databases and offsite facilities including the Internet at Level 4. Levels 3-4 have the capabilities for cyber security and cyber logging and generally use IP networks. There is another Level that could considered which is the "the Cloud." The process sensors and actuators operate almost exclusively in near-real-time (microseconds to milliseconds), whereas the HMIs (operator displays) provides information on the order of seconds to minutes. Sensors and actuators can operate, and in most cases were designed to function, without the IP network. In fact, following a 2015 Russian hack of the Ukrainian electric distribution network,[9] the electric distribution system was operated for months without the IP network as the network could not be trusted.

Figure 3 illustrates the equipment and information flows of a typical process system from the Process (Purdue Reference Model Level 0) to the Enterprise Resource Planning (ERP) systems (Purdue Reference Model Level 4). Generally, the Demilitarized Zone (DMZ) server resides at Level 3.5—the interface between the control and business networks. Technology has moved the intelligence down to lower level devices, enabling modern smart sensors to not only sense, but, , to also serve as PLCs and gateways. Since they are equipped with Ethernet ports, these smart digital sensors can communicate directly to the Internet or the Cloud, bypassing the Level 3.5 DMZ. This capability, which provides improved productivity, also introduces significant cyber risk as many digital sensors have built-in backdoors to permit calibration and other maintenance without a firewall, authorization, or authentication.

This article examines control system cyber security needs in the context of differences in how engineers and cyber security specialists generally tend to approach the subject. Variations in perspective are discussed and the nature and extent of control system cyber security threats are addressed. The paper then provides recommendations on how to upgrade the cyber security of control systems through technological, organizational, and educational approaches.

8 https://www.networkworld.com/article/3239677/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html

9 https://www.justice.gov/opa/press-release/file/1328521/download

Discussion

One of the primary differences between IT cyber security and control cyber security is the latter's need to protect life, physical property and the environment. Level 0, 1 sensors are like the feelings in fingers and toes. They provide stimuli to the brain, which is the control system. If the sensing inputs to the brain are impaired for any reason, the brain's actions will be incorrect. For example, if fingers are insensitive to a nearby flame, the brain will not react to pull fingers away. In the physical world, sensors measure pressure level, flow, temperature, voltage, current, strain, color, humidity, vibration, volume, chemistry, etc. These measurements are input to control systems such as PLCs, electrical breakers, motors, etc., which are programmed to maintain systems within physical constraints based on appropriate sensor readings. These readings are assumed to be uncompromised, stable, and accurate. However, manipulation of these devices by cyberattack, hardware back doors or insider or physical manipulation, whether unintentionally or maliciously, can have catastrophic consequences.

The February 2017 NASA Inspector General's report provided three case histories where IT technologies caused impacts or damage to control systems and operations. They illustrate the types of issues that can occur at a micro or macro scale.

- A large engineering oven that uses OT networks to monitor and regulate its temperature lost this ability when a connected computer was rebooted after application of a security patch update intended for standard IT systems. The reboot caused the control software to stop running, which resulted in the oven temperature rising and a fire that destroyed spacecraft hardware inside the oven. The reboot also impeded alarm activation, leaving the fire undetected for 3.5 hours before it was discovered by an employee.

- Vulnerability scanning used to identify software flaws that can be exploited by an attacker caused equipment to fail and loss of communication with an Earth science spacecraft during an orbital pass. As a result, the pass was rendered unusable and data could not be collected until the next orbital pass.

- Disabling of a chilled water Heating, Ventilation, and Air Conditioning (HVAC) system supporting a data center caused temperatures to rise 50 degrees in a matter of minutes, forcing shutdown to prevent damage to critical IT equipment.

Table 1 presents operational differences between IT and industrial control systems. These differences are compounded by how IT networking professionals and control system engineers approach the security issues in their purview. In many respects, they are fundamentally different (Table 2). Issues such as Zero

Trust vs 100% trust influence architecture, training, and policies. The difference between networking systems that are non-deterministic and control systems that are deterministic directly affects technology and testing. This has resulted in control systems having been shut down or sometimes damaged by using inappropriate network technology or testing tools including in the cases discussed above.

Table 1. Summary of IT System and ICS Differences

	Information Technology System	Industrial Control System
Performance Requirements	Non-real time Response must be consistent High throughput demanded High delay and jitter may be acceptable Less critical emergency interaction Tightly restricted access to control can be implemented to the degree necessary for security	Real time Response is time critical Modest throughput is acceptable High delay and/or jitter is not acceptable Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (Reliability) Requirements	Responses e.g. rebooting are acceptable Availability deficiencies can often be tolerated depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing
Risk Management Requirements	Manage data Data confidentiality is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Control physical world Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime may not be acceptable Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment or production
System Operation	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools	Differing and possibly proprietary operating systems, often without security capabilities built in Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
Communications	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices	Many proprietary and standard communication protocols Several types of communications media used including dedicated wired and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days or weeks in advance. ICS may use OSs that are no longer supported
Managed Support	Allow for diversified support styles	Service support usually via a single vendor
Component Lifetime	Lifetime in the order of 3 to 5 years	Lifetime on the order of 10 to 15 years
Components Location	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

US Department of Commerce, National Institute of Standards and Technology. "Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, Rev 2, May 2015, pp. 2-16, 17.

Table 2. Differences Between Networking and Engineering

IT/OT (Networking)	Engineering
Zero trust	100% trust
Part of cyber security teams	Generally, not part of any cyber security team
Worried about vulnerabilities	Worried about process and equipment
IP networks with security	Lower level non-IP networks without security
Assume all communications go thru IP network	Can get to Level 0,1 without IP network
Vulnerability assessments required	Level 0,1 not applicable
Non-deterministic	Deterministic
Worried about Advanced Persistent Threats	Design features with no security
Focus on malicious attacks	Focus on reliability/safety

The ability to implement suitable control system cybersecurity measures should rest, in part, on accurate information regarding sensor measurements, actual control system infiltration attempts, and system accidents which could be cyber-related. Unfortunately, cyber forensics are extremely limited for Level 0, 1 devices, nor is there adequate cyber security training at this juncture for the majority of control system engineers. There has been reticence by government organizations both within the U.S. and internationally to share information about control system cyber incidents. Control system and equipment vendors are often made aware of control system cyber incidents with their equipment but do not share the information because of non-disclosure agreements. Consequently, there has been minimal identification or disclosure of actual control system cyber incidents. Even though there is a continuous flow of cyber vulnerability disclosures of Level 2 on up, there have been no cyber vulnerability disclosures by the DHS ICS-CERT on Level 0, 1 devices.

This is true regarding Supervisory Control and Data Acquisition (SCADA) systems,[10] which are central to the integrity and performance of critical infrastructures. "The escalating sophistication and modernization as well as real time con-

10 https://www.inductiveautomation.com/resources/article/what-is-scada

tinuous operation and distributed, multi-component architecture underpin the growth of cyber threats to SCADA systems ... they are exposed to a wide range of cyber threats also because of the standardization of communication protocols, growing interconnectivity and legacy" (Cherdantseva, 2016). The same can be said of plant Distributed Control Systems (DCSs) used in power plants, refineries, chemical plants, water treatment systems, etc. which is the rationale behind the Open Process Automation Initiative.[11]

Perhaps the biggest hole in SCADA, DCS, and other control systems can be traced to connectivity to both internal business systems and external partners.[12] While business processes are made more efficient, the concentration of IT assets and streamlined networking of control system and IT processes leaves control systems vulnerable to viruses, denial of service attacks, and malicious software (Lewis, Ted, 2020). It should also be noted that many legacy plant DCSs and SCADA systems may not be capable of running anti-virus or other cyber security programs.

Sample control system threat vectors are presented in Table 3. Several threats may be implicated in a single attack and operating issues may be mistaken for unintentional events or equipment "glitches." For example, Level 1 devices such as temperature transmitters provide input to controllers and HMIs to reliably monitor and safely control a process. These sensors are common in turbine/generator systems to provide input about unstable or unsafe conditions or provide safety shutdowns. They are integral to equipment operation and cannot be bypassed. If the sensors are out of accepted operating limits whether accidentally or maliciously, a turbine or generator may be prevented from starting. The lack of generator availability could, and has, caused grid outages affecting large numbers of electricity consumers.[13]

One window on the current scale and future potential of control system attacks can be found in control system cyber security surveys. For example, the Claroty assessment of 365 ICS vulnerabilities was published by the National Vulnerability Database (NVD). During the first half of 2020, 53 venders received 139 ICS advisories issued by the Industrial Control Systems Cyber Emergency Response Team (IC-CERT.[14] 1H ICS vulnerabilities published by the NVD (2019) increased by 10.3% from 331, while ICS-CERT advisories increased by 32.4% from 105. More than 75% of vulnerabilities were assigned high or critical Common Vulnerability Scoring System (CVSS) scores. According to the report, more than 70%

11 https://www.opengroup.org/forum/open-process-automation-forum

12 IT can be backed up and restored, but process degradation can result in a physical mess that must be cleaned up. This results in a culture of greater risk taking in IT that would not be accepted by Engineers.

13 Texas PUC Docket-40368

14 "Most ICS vulnerabilities disclosed this year can be exploited remotely", Industry News, August 20, 2020, https://www.helpnetsecurity.com/2020/08/20/ics-vulnerabilities-exploited-remotely/

of the vulnerabilities published by the NVD can be exploited remotely, reinforcing the fact that fully air-gapped ICS networks that are isolated from cyber threats have become vastly uncommon.

Table 3. Control System Threat Vectors

Control Room Info Delay/Blockage	Disrupting the operations of control systems by delaying or blocking the flow of information through supporting networks, thereby denying availability of these networks to control system operators and production control managers.
Alter structures, thresholds, or commands	Attempting to or succeeding in making unauthorized changes to programmed instructions within PLC, RTU, or DCS controllers, change alarm thresholds, or issue unauthorized commands to control station equipment, which could potentially result in damage to equipment (if tolerances have been exceeded), premature shutdown of processes (shutting down transmission lines or causing cascading termination of service to the electrical grid), or disabling control station equipment.
Send falsified info to operators	Sending falsified information to control system operators, either to disguise unauthorized changes or to initiate inappropriate actions to be taken by systems operators that is, falsified information is sent or displayed back to system operators who may think that an alarmed condition has been triggered, resulting in system operators acting on this falsified information, thus potentially causing the actual event.
Modify software or firmware	Modifying or altering control system software or firmware such that the net effect produces unpredictable results (such as introducing a computer "time bomb" to go off at midnight every night, thus partially shutting down some of the control systems, causing temporary brownout condition; a "time bomb" is a forcibly introduced piece of computer logic or source code that causes certain courses of action to be taken when either an event or triggered state has been activated).
Safety system interference	Interfering with the operation and processing of safety systems (e.g., tampering with or denial of service of control systems that regulate processing control rods within a nuclear power generation facility).
Remote facility control system penetration	Many remote locations containing control systems (as part of an enterprise DCS environment) are often unstaffed and may not be physically monitored through surveillance; the risk of threat remains and may be higher if the remote facility is physically penetrated at its perimeter and intrusion attempts are then made to the control systems' networks from within.
Miscellaneous	Control systems are vulnerable to attacks of varying degrees ranging from telephone line sweeps (aka wardialing), to wireless network sniffing (wardriving) to physical network port scanning and physical monitoring and intrusion.

The potential for remote exploitation has been exacerbated by a rapid global shift to a remote workforce and the increased reliance on remote access to control system networks in response to the COVID-19 pandemic. The energy, critical manufacturing, and water & wastewater infrastructure sectors were by far the most impacted by vulnerabilities published in ICS-CERT advisories. Of the 385 unique Common Vulnerabilities and Exposures (CVEs) included, energy had 236, critical manufacturing had 197, and water & wastewater had 171. The research team discovered 26 ICS vulnerabilities disclosed during the first half of 2020, emphasizing critical or high-risk vulnerabilities that could affect the availability, reliability, and safety of operations.

ICS honeypots[15] have demonstrated that control system networks and devices are being targeted. In 2013, Trend Micro released research on a honeypot for a water system that mimicked a real system, including a human-machine interface (HMI) and other components of an ICS. In that research, there were 12 targeted attacks out of 39 total attacks. From March to June 2013, TrendMicro observed attacks originating in 16 countries, accounting for a total of 74 attacks on seven honeypots within the honeynet. Out of these 74 attacks, 11 were considered "critical." Some were even able to compromise the entire operation of an ICS device.[16]

In 2015, TrendMicro released research around the Guardian AST monitoring system using a honeypot called GasPot, which simulated a gas tank monitoring system.[17] The purpose of this honeypot was to deploy multiple unique systems that did not look the same, but nonetheless responded like real deployed systems. The goal was to build a honeypot that appeared so real that not even a well-trained control systems engineer would be able to tell that it was fake without diving deeply into the system. It consisted of four PLCs from three different brands: one Siemens S7-1200, two Rockwell MicroLogix 1100 units, and one Omron CP1L. These PLCs were chosen for their popularity in the control systems market from around the world. Also, each PLC brand used a different protocol and was loaded with logic to perform specific and associated tasks that ran the manufacturing facility. These roles were agitator, burner control, conveyor belt control, and palletizer, which used in robotic arms. To make the manufacturing process realistic, incremental and decremental functions varied the feedback values, which imitated the starting and stopping seen in real motors and heaters. Random generator functions were also created to make slight fluctuations in the feedback values to simulate actual variations.

Not only are current attackers accustomed to encountering honeypots, but advanced actors typically perform in-depth investigation before attacking a target system to make sure that they are not identified. For this reason, the honeypot not only needed to look realistic from a design and technical implementation standpoint, but it also had to reflect a system that a real company would use. The manufacturing honeypot went online in May 2019. For seven months, TrendMicro maintained the image of a real company and monitored the honeypot closely. The first attack encountered came a month after the honeypot went live, with several others following in its wake. This showed this sophisticated honeypot designed as a small business with critical clients and inadequate security was effective in luring threat actors.

15 A security mechanism to virtually lure attackers to exploit vulnerabilities in intentionally compromised computer resources to understand attack patterns, investigate breaches and achieve other goals.

16 https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-scada-that-didnt-cry-wolf.pdf?_ga=2.133698510.197023676.1601743116-943111934.1601743116

17 https://www.trendmicro.com/en_us/business/solutions/iot/smart-factory.html

During the May to December 2019 research period, it became apparent that there was increasing activity on the honeypot, with progressively higher interactions. The longer the honeypot was exposed, the more activity was observed—and the more sophisticated attacks appeared to be compared to standard penetration-testing techniques. This approach also demonstrated the need to have different parties (e.g., network security, engineering, etc.) involved.

Problem Scope

Complementing the discussion above, Dragos' Robert Lee states the following comment about defending control system networks:

> Advanced adversaries are dangerous because they have well-funded, focused, and determined personnel on their teams. They have the time and resources available to them to research a target and move past the mindset of single incidents and breaches into conducting full campaigns. These campaigns can take months or years to execute and, due to cultural and technical barriers within organizations, they often go unnoticed. The adversary may have the tools and tactics available to them, but their greatest strength is in their personnel. The only way to counter these human operators is with well-trained and empowered defenders. Defenders must also move past single intrusions to thinking about defense as a campaign as well—they must utilize a strategy." (Lee, Robert, 2020)

While there is no publicly available database of control system cyber security breaches, numerous examples have been reported. Many emerge in journalist accounts with cross referenced information sourcing. The record includes abortive attempts to impact infrastructure. As an example, the site acceptance testing of a Chinese-made transformer at the Western Area Power Administration's Ault substation outside of Denver in 2019 identified electronics that should not have been part of the transformer—hardware backdoors. It is probable that an adversary does not install transformer backdoors to steal data, but rather to enable remote control that could cause damage at a future time. As previously noted, a 345/230 kV Chinese transformer weighing over 500,000 pounds arrived at the Port of Houston in summer 2019. It was scheduled for installation at a US electric utility. Instead, it was trucked under Federal escort to a national laboratory due to the security concerns (Wall Street Journal, May 27, 2020). To date, there has been no information on what has been found.

This incident, along with threats involving other state actors, led to the May 1, 2020 issuance of Presidential Executive Order (EO) 13920: "Securing the United States Bulk-Power System."[18] The Executive Order states that "foreign adver-

18 The bulk power system does not generally include facilities used in local electrical energy distribution.

saries are increasingly creating and exploiting vulnerabilities in the United States bulk-power system, which provides the electricity that supports our national defense, vital emergency services, critical infrastructure, economy, and way of life." In addition to other provisions, the ER directs the Secretary of Energy, in consultation with the heads of other appropriate agencies, to "establish and publish criteria for recognizing particular equipment and particular vendors in the bulk-power system electric equipment market as pre-qualified for future transactions; and may apply these criteria to establish and publish a list of pre-qualified equipment and vendors." In addressing these concerns at the organizational level, the equipment and device vulnerabilities identified in the EO require that engineering be integrally involved (and preferably in the lead), not only the chief information and security officer (CISO) or control system security team.

Maintaining accurate and actionable databases of both successful and unsuccessful attacks is essential at the national scale. The OT Cyber Security Alliance compiled nine incidents from 2015-2019, including a blast furnace in a German steel mill suffering massive damage following a cyberattack and the Locker Goga ransomware attack that halted production at global aluminum manufacturer Norsk Hydro (OTCSA, 2019). Lewis relates ten major incidents involving SCADA systems, including the 2003 slammer worm infection of at least five power utilities. One impact was the disabling of a Davis-Besse Nuclear Power Station's monitoring system for nearly five hours (Lewis, 2020). Fortinet describes an attempted State-sponsored infiltration of up to 24 U.S. utilities between 2016 and 2018. An FBI investigation found that utility targets included those providing power to strategic defense facilities, and companies servicing utility industrial control systems (Fortinet, 2019).

A Temple University research team maintains a publicly accessible repository of critical infrastructure ransomware attacks (CIRWA) using Department of Homeland Security infrastructure categories. As of August 2020, over 680 attacks were recorded, with government installations being the most targeted critical infrastructure.

As of August 2020, this author has curated a database of more than 1,250 control system cyber incidents resulting in physical impacts (Table 4). They include both accidental incidents and those likely to have been caused by malign actors. A number of the incidents recorded were provided in confidence, which is why the database is not public. The cases are global in reach, including power (nuclear, fossil, hydro, renewables), electric transmission and distribution, water/wastewater, pipelines, manufacturing, transportation, space, and defense. The impacts range from trivial to substantial, including large-scale equipment damage and widespread blackouts. By my estimation, there have been more than 1,500 deaths directly related to the incidents and, more than $70 billion in cumulative damages to date.

The July 23, 2020 NSA/DHS CISA Alert AA20-205A: *Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems* (reference 10) stated that control systems should not be connected directly to IT networks or the Internet or they will be compromised. However, as of 2014, there were more than 2 million control system devices directly connected to the Internet and counting (Radvanovsky, 2014).

Attackers are becoming better system engineers than the defenders as they generally don't have organization charts or professional silos. It can be surmised that sophisticated attackers work "backwards" by determining what damage they want to cause and then look for tools to achieve that end.

Table 4. OT Cyber Security Incident Database

Incident Category	Count
Malicious	**416**
Insider	72
External	339
Other	5
Targeted	**183**
Loss of View	**759**
Loss of Control	**743**
Injury/Death	**95**
Equipment Damage	**154**
Environmental Damage	**116**
Sensor Involvement	**67**
Operational Impact	**905**
Entity or Sector	**Count**
Aircraft	**88**
Chemical Plant	**30**
Electric T&D/SCADA	**228**
Facilities	**62**
Food/Beverage	**19**
Land Transportation	**104**
Manufacturing	**97**
Marine	**33**
Medical	**25**
Mining	**9**
Nuclear Plants	**102**
Oil/Gas	**96**
Paper Production	**9**
Pipelines	**51**
Power Plants	**11**
Space	**49**
Water/Wastewater	**90**

Recommendations

There has been a convergence of highly integrated industrial automation sharing more constructs with IT, known as IT-OT (Operational Technology) convergence. It is the inevitable result of industry seeking higher efficiencies and productivity through physical and cyber control system convergence. General Electric, which has called this development the emergence of the "Industrial Internet," characterizes it as "where the Internet intersects with our basic human needs, such as water, transportation, healthcare, and energy."[19] This impending transition—which will increasingly drive most critical infrastructures—heightens the need for a correctly scaled national effort capable of meeting the security and safety needs of critical infrastructure control systems. As opposed to IT security, control system cyber security is still in the early developmental stages.

19 Also called the "Industrial Internet of Things (IIoT)," it should not be confused with the Internet of Things (IoT) which tends to refer to consumer products and devices.

As argued here, from the standpoint of infrastructure resilience, control system cyber security should not be regarded as a domain of limited importance, or simply as an extension of existing cyber security activities. In both new equipment design and legacy retrofits, cyber threats may not be sufficiently considered. It is fundamentally important to recognize access points to and from control systems because this is where incursions may be targeted, and where anomaly detection may prove fruitful.

Across the world, attempts are being made to grapple with the cyber security requirements of control systems in a context of both increasing system interconnectedness and heightened cyber risk. It is likely that promising advances will be made in both proactive and adaptive techniques to detect and mitigate control system cyber-attacks. Strategies include but are not limited to machine learning anomaly detection, advanced moving target and deception techniques, and consequence-based resilience architectures such as Consequence Driven Cyber-informed engineering (CCE).

In describing the latter approach, St. Michel and Freeman (2019) note that CCE is reliant on "the ability to merge cyber security experience and analysis with a level of engineering expertise that typically has not been included in the conversation. When assessing the technical impact, the (engineering) subject matter expertise is invaluable for not only determining the impact a single component level but also discovering how that exploitation will impact operations across an infrastructure or region."

In this light, it us useful to adapt an insider threat vector approach to anticipate both internal and external threats—how a party with destructive intent and knowledge of control system capabilities, plant operations, etc. can cause disruption of safety or other processes to damage critical infrastructure. At the equipment level, there is a need to assess the design and operation of these systems. An example is a turbine system with a turbine lube-oil pump. The turbine should never be operated without the lube-oil pump activated. At the design stage, the thought that this would intentionally happen may not have been considered. Rather than try to prevent this from a cyber perspective, which introduces more complexity, a design change of installing a mechanical interlock that automatically shuts the turbine down if the lube oil pump is out-of-service can prevent a safety issue from occurring. There are many examples where relatively simple changes of this nature can prevent a cyber or physical attack from causing damage. Obviously, this requires the participation of the engineering community from the design through operational stages.

One general solution holds great promise because it has the potential to provide additional cyber security, 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 inac-

curate or compromised, situational awareness is suspect. Monitoring changes in the electromagnetic spectra of Level 0, 1 devices could detect sensor anomalies, whether unintentional or malicious.[20] Specifically, such technology could determine the origin of the sensor signal which provides signal authentication. This can address the concerns identified in transformer hardware backdoors. The technology could also distinguish between ostensibly identical sensors which can go a long way towards identifying counterfeit devices that include communication and spoofing capabilities. The validity (and implicit authentication) of these devices would be strengthened by monitoring their electromagnetic spectra and electrical signal characteristics over time.

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

Control System Cyberattack Transparency

There are, as noted, a limited number of control system manufacturers serving the majority of industries globally. Security sometimes includes common passwords that cross industries and continents. There are also a finite number of major system integrators who also work across industries. Control system vendor users' groups are often open with common information sharing portals. It should be evident there is dissemination of control system knowledge that is accessible by both defenders and attackers.

Older control system vulnerabilities may be sufficient to gain entry and cause the desired impacts. Defenders often focus on the latest network attacks without considering the physical impacts that may or may not be created. Consequently, there is a need to understand and adapt to the myriad approaches that attackers are using. There is also understandable reluctance to make information about control systems broadly available because of concern about adversaries. But this reticence to share information can hurt defender capabilities, as attackers will be driven to seek the latest information.

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) vision on securing ICS includes an "ICS community faster and smarter than its adversaries, where (the community) raises the cost, time and complexity thresholds for successful ICS attacks to the point that they exceed the capabilities of even the most advanced threat actors" (CISA,

20 Lopez, J, Perumall, K., & Yoginath,S. "Detecting Sensors and Inferring their Relationships at Level-0 in Industrial Cyber-Physical Systems," Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), November 5-6, 2019.

2020). Can this occur sufficiently and in time to avert the magnitude of challenges ahead? Beyond EO 13920, this question should be granted primary national security importance.

It is arguable that some attackers are becoming better system engineers than the defenders since they generally don't have organizational charts with the resultant silos. It may prove difficult for defenders to stay ahead of attackers. Sophisticated attackers often work backwards by determining the damage they want to cause and then producing tools to achieve that goal. "Some attackers are highly organized professional teams executing targeted and disruptive attacks with sophisticated tools for ransom, revenge, or worse. Many are well funded, especially when sponsored by nation states."[21] "Today, the big prize, the *piece de resistance* of cyber malfeasance, is the industrial sector full of systems that were not designed with security in mind ..."[22]

The paradoxes of providing cyber security in most settings are well known. There is "a complex ecosystem in a cyberphysical society. Ignorance, a limited understanding of what needs to be done, limited awareness of the issue despite its significance and urgency, have resulted in a lack of action, planning and policies" (Bruijn, 2017). This makes it essential to continuously estimate the potential costs, benefits and risks of sharing rather than concealing information that is pertinent to OT cyber security. In most instances, a deft assessment of concealing threat intelligence versus supplying the necessary facts to defenders will need to be made. However, in terms of national security, the expanding attack surface associated with control system security will increasingly require that timely determinations be made.

In this context, the CISA *Unified Initiative: FY 2019-2023* needs to be broadly supported, appropriately resourced, and led. Most importantly, it needs to be vigorously evaluated in terms of the nature and scope of control system resilience built through the program. Organizations such as the US General Accountability Office (GAO) and the National Academies of Sciences, Engineering and Medicine have the resources to constructively evaluate progress.[23]

Organizational Culture and Skills

Culture and governance issues are critical to securing control systems. However, as argued, the prevailing governance model is such that cyber security is viewed as a network, not an engineering problem. For control system security, this is a barrier that needs to change. The engineering component of organizations is generally re-

21 General Electric, 2017, p. 21.

22 Ibid, p. 20.

23 "Securing Industrial Control Systems: A Unified Initiative, FY2019-FY2023," Cybersecurity and Infrastructure Security Agency, July 2020. See https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf

sponsible for control system equipment and understands how these systems work and interact. Many network security-induced control system cyber incidents have occurred because of inadequate coordination. Several examples are provided.[24] Moreover, in this author's opinion, very critical cyber events such as the Aurora Generator Test have not been adequately addressed because engineering expertise has not been sufficiently involved.[25]

Change will not happen unless government-run critical infrastructures and privately held infrastructure CEOs make smart determinations about the need for improved control system security across their operations—and incorporating that recognition in the corporate culture. When one considers that current defenses may be inadequate to avert a control system failure, issues of service disruption, inherent risk, severe accident occurrence, control compliance, facility damage and remediation and community relations can come into play. This risk has been identified by Moody's Investor Services as a concern in several recent presentations and in response to Executive Order 13920.[26]

The cultural gap between the cyber security and engineering teams starts at the university level. The impact of this gap is reflected in the disparity of engineering systems vs cyber security product designs, to the extent that they diverge rather than converge. Understanding and mitigating control system attacks requires operators, researchers and technicians to have access to extensive theoretical and practical knowledge. Control system cyber security is an interdisciplinary field that should encompass computer science, networking, public policy, and engineering control system theory and applications. Unfortunately, today's computer science curriculum typically does not address the unique aspects of control systems. At the same time, electrical engineering's power system focus, and chemical engineering, mechanical engineering, nuclear engineering, and industrial engineering curricula, do not adequately address computer security. There is a need to formulate and implement interdisciplinary programs for control system cyber security both in the university setting as well as through industry-supported onsite and supplementary educational opportunities.

It is useful to conceptualize how control cyber security is situated relative to the IT security and the control systems engineering frames. As Figure 4 indicates, the vast majority of individuals working in this space are from the IT world, with a subset dedicated to IT security. Movement must occur at the intersection of IT security and control systems engineering in order to enable constructive dialogue,

24 Industrial Control System Security Within NASA'S Critical and Supporting Infrastructure, February 8, 2017, NASA Report No. IG-17-011, https://oig.nasa.gov/audits/reports/FY17/IG-17-011.pdf

25 https://www.controlglobal.com/blogs/unfettered/not-all-cyberattacks-are-malware-incidents-it-didnt-take-any-lines-of-code-to-blow-up-a-27-ton-generator

26 Moody's Credit Outlook, "US electric utilities will benefit from cybersecurity measures in executive order," May 6, 2020.

joint planning and a holistic organizational response for OT cyber security improvement.

At the national level, given the massive movement underway towards AI, IoT, and the industrial internet, there is a need to accelerate implementation of university programs as well as mid-career training opportunities: to acclimate engineers to IT issues and to train IT practitioners to control system realities including unique issues such as latency, jitter, and other control system-unique issues that can have detrimental impacts on the process.

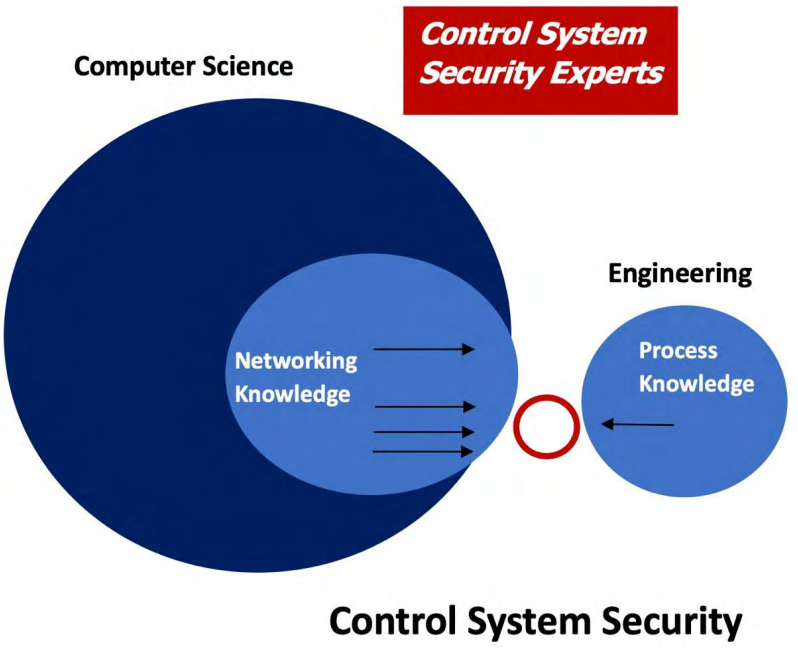

Figure 4. Control System Security Practitioners

For example, in university Computer Science and Engineering programs, consideration should be given to an area elective in Control System Cybersecurity. In addition, Control System Cyber Security could be offered as a course elective within Communications and Networks, Information, Software and Systems and Security, and other concentrations.

It is necessary to develop control system cyber security training for practicing engineers. The goal would be to expand the skills base in control system operations and engineering with a basic understanding of control system cyber security defenses and realistic mitigation efforts. This training would include addressing control system Level 0, 1 field devices as well as addressing actual control system cyber incidents.

In addition, models involving force multipliers for engineers in control system settings might be explored. In response to an acute need for healthcare in

the mid-1960s, a number of groups, including the American Medical Association, were instrumental in establishing a new class of medical provider: the Physician Assistant (PA). From four initial U.S. Navy Hospital Corpsmen, there are approximately 140,000 PAs in the United States today (National Commission, 2019). Typically working under the direction of a medical doctor, PAs are in great demand in physician offices, hospitals, outpatient clinics and other healthcare settings.

Based on the acute need for operating system cyber-security across the nation's sixteen critical infrastructure sectors, there may be reason to evaluate the potential to create a new engineer extender responsible for control system security. An Engineer Assistant (EA) with training and certification necessary to advance control system security could be applied in diverse settings across sectors. In addition to physical asset security, such personnel would be acclimated to the cybersecurity of control systems. Organizations such as the American Society for Engineering Education (ASEE), the National Society of Professional Engineers (NSPE), the International Council on Systems Engineering (INCOSE), the International Society of Automation (ISA), and the Institute of Industrial Engineers (IIE), and other relevant groups might determine the efficacy of advancing this type of goal.

In any strategy to improve the workforce focused on OT cyber security, technical advances promise to permit cost effective learning experiences. The price of even modest control systems can range into hundreds of thousands of dollars. ICS emulators and modern software learning systems have the capacity to efficiently train large numbers of practitioners.

Appendix: Control System Cyber Security Definitions

The terms IT, OT, and IT/OT convergence come from the ISA TS12 Industrial Networking and Security course.

Information Technology (IT)—The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.

- Operational Technology (OT)—Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events (Gartner, 2020). OT is not the pumps, valves, or other hardware nor does it include the engineers and technicians responsible for the equipment.

- IT/OT Convergence—The integration of IT technology with OT systems.

- Cyber Incident—The defacto IT definition of a cyber incident is a computer system connected to the Internet, running Windows, and data is maliciously manipulated or stolen. It is about privacy. The NIST definition is an occurrence that actually or potentially jeopardizes the **C**onfidentiality, **I**ntegrity, or **A**vailability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional (FIPSPUB 200, 2006). Note there is no mention of "malicious" or safety. Also note that for control systems, I and A are much more important than C.

- "Smart" Cities, grid, sensors, manufacturing, water .... Smart means two-way communications and programmable and includes Industry4.0 and Industrial Internet of Things (IIoT). All of these technologies are cyber vulnerable.

Author Capsule Bio

Joseph Weiss is an expert on instrumentation, controls, and control system cyber security. He has published over 80 papers, 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 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.

References

Basnight, Zachry. 2013. "Firmware Counterfeiting and Modification Attacks on Programmable Logic Controllers. Thesis: Department of Electrical and Computer Engineering, Graduate School of Management, Air Force Institute of Technology.

Butterworth, Jim. 2016. *Threat Vectors*. In Radvanovsky & Brodsky. Taylor & Francis Group.

Butts, Jaromin, Mullins, Barry, Butts, Jonathan, & Lopez, Juan. 2013. "Design and Implementation of Industrial Control System Emulators." In Butts and Shenoi (Eds.) *Critical Infrastructure Protection VII, IFIP AICT 417*, pp. 35-46.

Chavez, Adrian. 2019. "Moving Target Defense to Improve Control System Resiliency." In Rieger et al. (Eds.), *Industrial Control Systems Security and Resiliency, Practice and Theory*. Springer, pp. 143-167.

Cherdantseva, Yulia, Burnao, Pete, Blyth, Andrew, Eden, Peter, Jones, Kevin, Soulsby, Hugh, & Stoddart, Kristan. 2016. "A Review of Cyber Security Risk Assessment Methods for SCADA System." *Computers & Secu*rity 56, pp. 1-27.

Cybersecurity and Infrastructure Security Agency (CISA). 2020. *Securing Industrial Control Systems: A Unified Initiative FY2019-202.*

Executive Order 13920. May 1 2020. "Securing the United States Bulk Power System." *Federal Register*, Vol 8, No. 86.

FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information System*, March 2006.

Fortinet. 2019. *A Solution Guide to Operational Technology Cybersecurity*, pp. 1-24.

Gartner Information Technology Glossary. 2020. https://www.gartner.com/en/information-technology/glossary.

General Electric. 2017. *An Executive Guide to Cyber Security for Operational Technology*, pp. 1-29.

Glenn, Colleen, and Sterbentz. 2016. "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. *Idaho National Library*.

Glover, J Duncan, Overbye, Thomas, & Mulukutla, Sarma. 2017. Power System Analysis & Design. Cengage Learning.

Lee, Robert. 2016. Active Defense in Industrial Control Systems. In Radvanovsky & Brodsky. Taylor & Francis Group.

Lewis, Ted. 2020. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Third Edition. John Wiley & Sons.

McJunkin, Timothy, Rieger, Craig. 2019. Resilient Control System Metrics. In Rieger et al. (Eds.), *Industrial Control Systems Security and Resiliency, Practice and Theory*. Springer, pp. 255-276.

Morris, Thomas, Vaughn, Rayford, & Dandrass, Yoginder. 2011. "A Testbed for SCADA Control System Cybersecurity Research and Pedagogy."

NASA. 2017. Industrial Control System Security Within NASA'S Critical and Supporting Infrastructure, Report No. IG-17-011.

National Commission on Certification of Physician Assistants. 2019. Statistical Profile of Certified Physician Assistants."

OTCSA White Paper. 2019. Introducing the Operational Technology Cyber Security Alliance.

Radvanovsky, Robert. 2014. Project Shine Findings Report Results, Presentation to the 2014 ICS Cyber Security Conference.

Pustogarov, Ivan, Ristenpart, Thomas, & Shmatikov. 2017. "Using Program Analysis to Synthesize Sensor Spoofing Attacks." Association for Computer Machinery.

Radvanovsky, Robert & Brodsky, Jacob. 2016. *Handbook of SCADA/Control Systems Security*. Taylor & Francis Group.

Rieger, Craig, Ray, Indrajit, Zhu, Quanyan, & Haney, Michael. 2019. (Eds.) *Industrial Control Systems Security and Resiliency, Practice and Theory*. Springer Nature Switzerland.

Saritas, Sirkan, Sandberg, Henrik, Dan, & Gyorgy. 2019. "Adversarial Attacks on Continuous Authentication Security: A Dynamic Game Approach." In: Alpcan, T. Vorobeychik, Y. Baras J., Dan, G. (Eds.) *Decision and Game Theory for Security*. GameSec 2019.

Shaw, Keith. 2018. The OSI model explained: How to understand (and remember) the 7-layer network model. *Network World*, October 22, 2018.

St. Michel, Curtis & Freeman, Sarah. 2019. "Consequence-Based Resilience Architectures." In Rieger et al. (Eds.), *Industrial Control Systems Security and Resiliency, Practice and Theory*. Springer, p. 22.

Stouffer, Keaiht, Pillitteri, Victoria, Lightman, Susan, Abrams, Marshall, & Hahn, Adam. May, 2015. Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, U.S. Department of Commerce.

Young, William, Leveson, Nancy. 2013. "Systems Thinking for Safety and Security." Proceedings of the *2013 Annual Computer Security Applications Conference* (ACSAC 2013), New Orleans.

Wall Street Journal. Smith, Rebecca. May 27, 2020. *U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny.*

Weiss, Joseph, "The Need for Interdisciplinary Programs for Cyber Security of Industrial Control Systems," WorldComp 2010, Las Vegas, NV.

Weiss, Joseph, "Attention Policymakers: Cybersecurity is More than an IT Issue," *PE Magazine*, May/June 2020.