A Current View of Gaps in Operational Technology Cybersecurity

Joe Weiss and Richard Ku

TREND MICRO™ | research

Published by

Trend Micro Research

Written by

Joe Weiss
Applied Control Solutions, LLC

Richard Ku
Trend Micro Incorporated

Contents

The purpose of control system cybersecurity is to protect the control systems and the processes they monitor and control from electronic threats — that is, to "keep lights on and water flowing." Networks are a support function in the overall objective of safety, reliability, and productivity — that is, to optimize the processes. What makes control system cybersecurity different from IT cybersecurity is the need to protect life and physical property. Because unintentional cyber incidents can be just as deadly and damaging as malicious events, both must be addressed.

Monitoring and preventing compromise of data has been an IT function since the late 1980s, while control system cybersecurity has been a major issue since 1998, with the signing of Presidential Decision Directive 63 in the US, which tackles critical infrastructure protection.[1]

Before 9/11, cybersecurity was simply one of the risks that had to be considered when designing and implementing control systems, including those for seismic, environmental, fire, and reliability concerns. As these were all engineering considerations, control systems were 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 in charge, and its function included cybersecurity. The focus was from the "bottom up." The main consideration was whether the process could be affected, which was essentially process anomaly detection or, in other terms, mission assurance.

After 9/11, cybersecurity became a matter of national security. It was at this time that the cybersecurity function for control systems was moved to the IT organization and engineering was no longer involved. Consequently, all cybersecurity monitoring and mitigation were at the IP (Internet Protocol) network layer — network anomaly detection. As a result, control system cybersecurity went from being mission assurance to information assurance.

Since engineering systems are not within IT's purview, control system devices — such as process sensors, actuators, and drives — still do not have capabilities for cybersecurity, authentication, or cyberlogging, nor can they be upgraded. Lower-level sensor networks — such as HART (Highway Addressable Remote Transducer),[2] Profibus,[3] and Fieldbus[4] — also have no cybersecurity.

The lack of focus on control system devices is still occurring. There is a need for cybersecurity to protect all the systems at all levels of the industrial control system (ICS) environment as the old adage that a breach arises from the weakest link applies to control systems. Moreover, because of the continuing profusion of ransomware attacks, there has not been the same focus on cyberattacks that could cause physical damage.

Glossary

The following are a few terms used in control system cybersecurity and their corresponding definitions. The terms *IT*, *OT*, *IT/OT convergence, and IoT* come from the ISA TS12 Industrial Networking and Security course.

Information technology (IT): This refers to the study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.

Operational technology (OT): This refers to hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events.[5] OT is not the pumps, the valves, or other hardware, nor does it include the engineers and the technicians responsible for the equipment.

IT/OT convergence: This refers to the integration of IT with OT systems.

Internet of things (IoT): This refers to the internetworking of physical devices (also referred to as "connected devices" or "smart devices") and other items embedded with electronics, software, sensors, and network connectivity, which enable these objects to collect and exchange data. The term mostly refers to consumer devices such as smart watches, smart printers, and smart cars.

Cyber incident: The de facto IT definition of a cyber incident is when a computer system is connected to the internet and is running Windows, and data is maliciously being manipulated or stolen. It is about privacy. The definition by the National Institute of Standards and Technology (NIST) is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (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.[6] It should be noted that there is no mention of "malicious" or safety. It should also be noted that for control systems, I and A are much more important than C.

Smart: When applied to things such as cities, grids, sensors, and manufacturing, this refers to two-way communications and programmability, and includes Industry 4.0 and industrial internet of things (IIoT). All of these technologies are cyber-vulnerable.

Cybersecurity

Cybersecurity became an IT issue after the first virus or worm was identified in the late 1980s. The Morris worm of Nov. 2, 1988 — usually considered the first computer worm and certainly the first to gain significant mainstream media attention — was distributed via the internet. This worm resulted in the first conviction in the US under the 1986 Computer Fraud and Abuse Act. IT cyberattacks have continued unabated, leading to widespread attention and legislation. IT cybersecurity threats have also led to the development of the cybersecurity industry — with companies like Trend Micro, McAfee, and Symantec — and cybersecurity policies — starting with ISO/IEC27000, which is part of a growing family of ISO/IEC information security management systems (ISMS) standards within the field of information and IT security. Standards include general methods, management system requirements, techniques, and guidelines for addressing both information security and privacy. However, these standards are IT-focused and do not address the unique issues associated with control systems, including reliability and safety. This has led to the establishment of ISA99, which is developing the suite of IEC 62443 series of automation and control system cybersecurity standards specific to automation and control systems, as illustrated in Figure 1.[7] And as digital transformation happens across many verticals and industries, other standards will also need to be updated to ensure that they can meet the cybersecurity challenges of these fast changing verticals and industries.

Figure 1. ISA/IEC 62443 control system cybersecurity standards

Control Systems

The Purdue Reference Model, shown in Figure 2,[8] was developed in the 1990s to identify information flows in control systems. Cybersecurity was not an issue for the reference model. The Purdue Reference Model was also based on the existing technology, which made discriminating between sensors, controllers, process control networks, and others straightforward as their capabilities were limited. With the microprocessor and communication revolution, the process reference model levels are no longer so straightforward as the technologies enable process sensors to also have programmable logic controller (PLC) capabilities and even communication gateway capabilities.

The Level 0,1 devices used in critical infrastructures are not cyber-secure. In fact, many instrumentation and low-level instrumentation networks may not be able to be secured. Levels 2 and 3 are critical to secure as they generally use traditional networking architectures to communicate with other control systems within the facility and can also communicate with the cloud.

The cloud level was not considered when the model was developed. It is currently being lumped within Level 5. Consideration should be given to creating a new level specifically for the cloud. This is especially important for verticals like manufacturing, healthcare, and retail as these are industries that seem to adopt cloud and virtualization faster than other industries like oil, gas, and power.

This is in contrast to the International Standards Organization (ISO) seven-layer model that was developed for network communications and security.[9] The ISO model divides network communication into Layers 1 – 4, which are considered the lower layers and mostly concern themselves with moving data around. Layers 5 – 7, called the upper layers, contain application-level data. Networks operate on one basic principle: “Pass it on.” Each layer takes care of a very specific job and then passes the data onto the next layer. This is exactly what occurs at the Purdue Reference Model 2 – 3 networks.

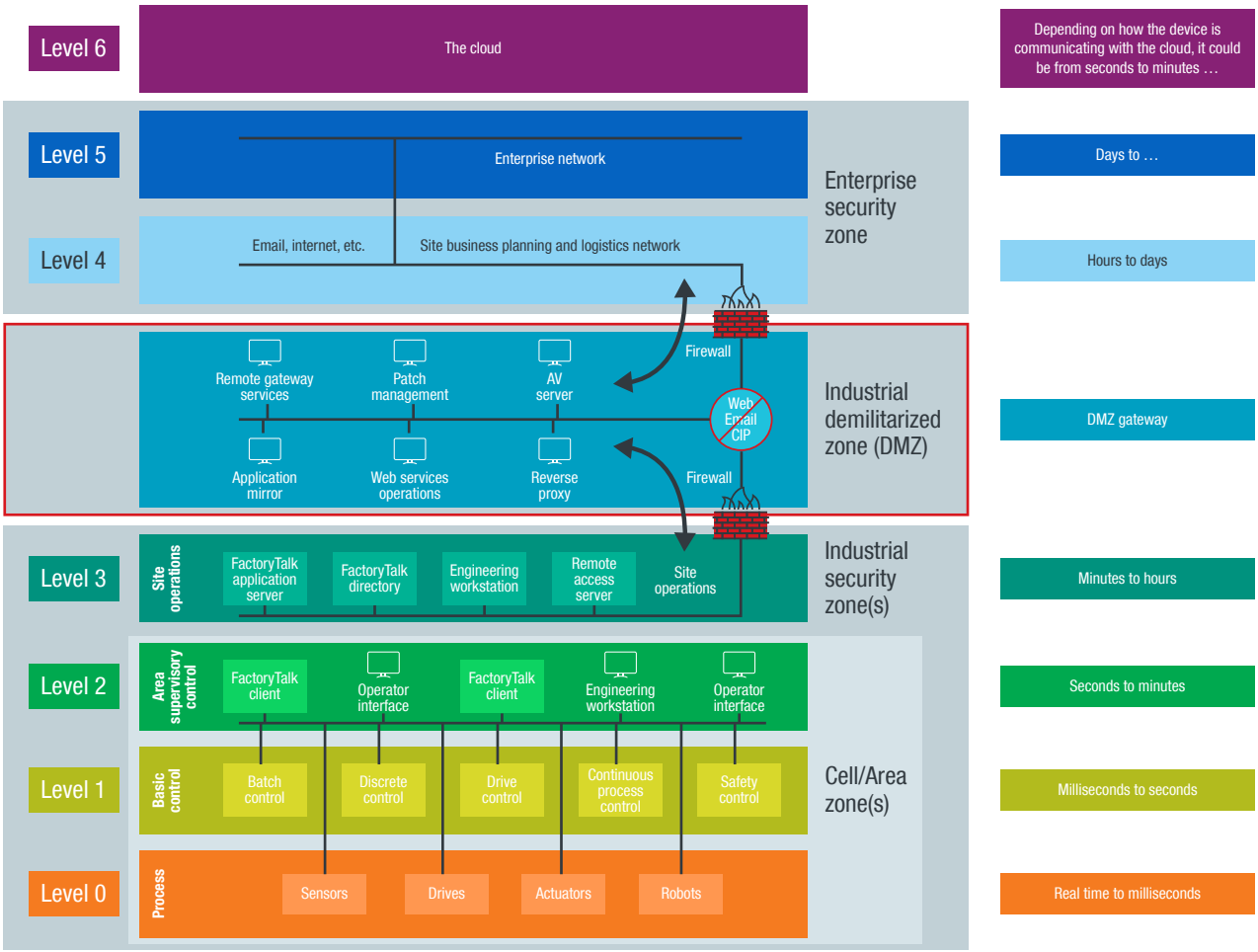


Figure 2. The Purdue Reference Model

A typical control system is composed of Level 0,1 devices (sensors, actuators, and drives) connected to Level 2 controllers that are connected to process control networks and human-machine interfaces (HMIs), also known as operator displays, at Level 3, which are connected to long-term databases and off-site facilities including the internet at Level 4. Level 3 – 4 have the capabilities for cybersecurity and cyberlogging, and generally use IP networks, as shown in Figure 2. The sensors and the actuators operate almost exclusively in near-real time (microseconds to milliseconds), whereas the HMIs provide operator information on the order of seconds to minutes. The sensors and the actuators can operate — and in most cases were designed to function — without the IP network.

Figure 2 provides a representation of the equipment and the information flows in 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 would reside at Level 3.5. However, as technology has moved the intelligence further down to the lower-level devices, modern smart sensors can act not only as sensors but also as PLCs and gateways since they are equipped with Ethernet ports that allow direct communication with the cloud or the internet, bypassing the Level 3.5 DMZ. This capability, which provides improved productivity, also introduces a very significant cyber risk

as the digital sensors have built-in backdoors to allow for calibration and other maintenance activities without a firewall or authorization.

As organizations transform their businesses with the adoption of the cloud and virtualization to help provide better visibility and improve productivity and efficiency, we believe there is a new level, Level 6: the cloud, which needs to be considered for cybersecurity.

Figure 3 shows how business risk and cyberthreats are directly connected, and we have seen this risk model proved to be correct over that last several decades across the several big transformations — from client/server architecture, to LAN/WAN architecture, to the internet architecture to the cloud/SaaS/ container architecture, and now to the convergence of IT/OT and the OT digital transformation architecture.

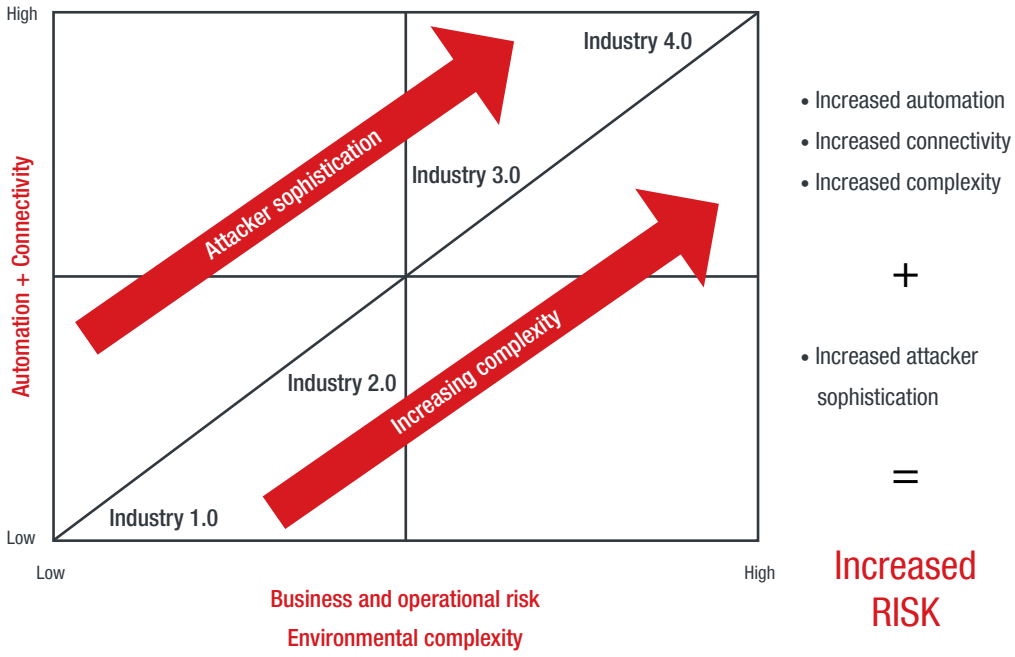


Figure 3. Evolution of industrial cyber risk

Control System Cybersecurity

In order to understand the cybersecurity status of an organization's OT and control system environment, an example of which is shown in Figure 4, there is a need to understand how the control systems interact with the different threat vectors that could potentially affect their OT environment.

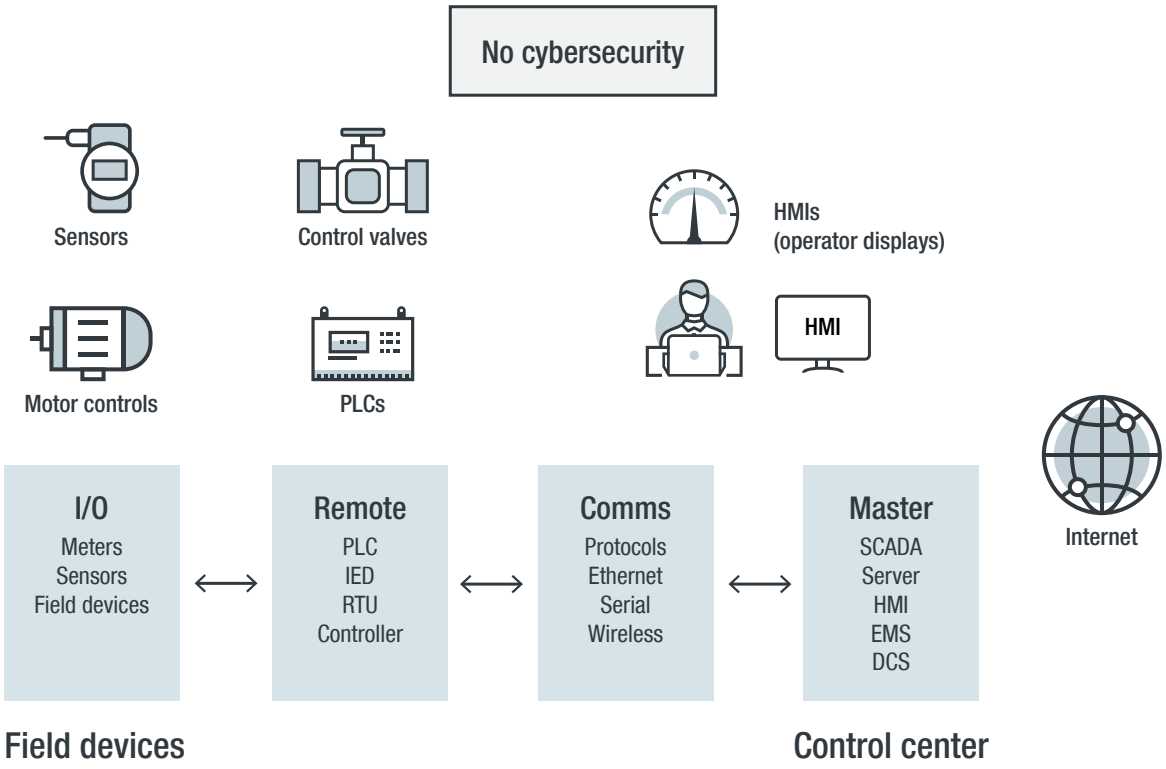


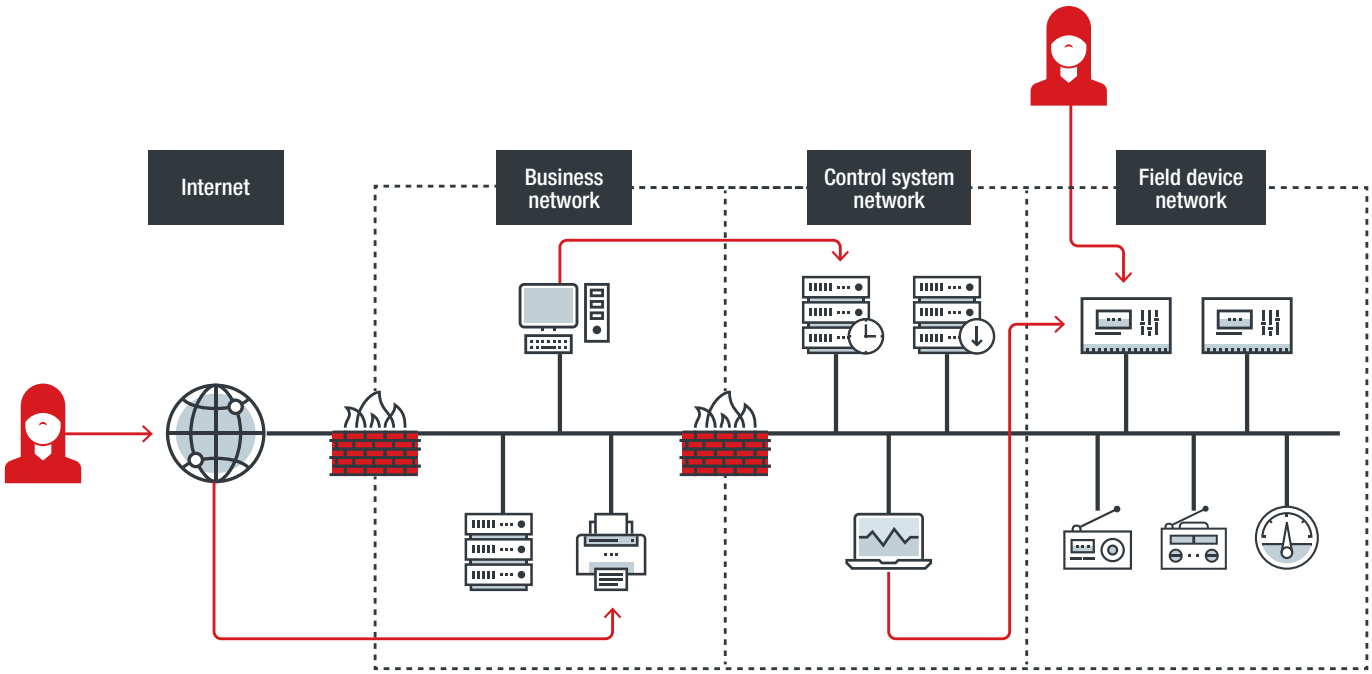
Figure 4. A typical organization's OT and control system environment

The Level 0,1 sensors are like the feelings on our fingers and toes. They provide the stimuli to our brains, which are the control system. If the sensing input to our brains are wrong for any reason, the actions of the brain will not be correct. For example, if our fingers are insensitive to a flame near our fingers, the brain will not react to pull our fingers away from the flame. In the physical world, sensors measure pressure, level, flow, temperature, voltage, current, strain, color, humidity, vibration, volume, chemistry, and other parameters. The measurements are input to control systems such as PLCs and electrical breakers, which are programmed to maintain systems within physical constraints based on sensor readings. The sensor readings are assumed to be stable and accurate. Consequently, calibration intervals are generally scheduled every 1 to 3 years to "recorrect" the sensor readings as they "drift" over time.

In the 1970s through the mid-1990s, sensors and control systems were isolated systems not connected to the outside world. They were entirely within the purview of the engineers who designed, operated, and maintained these systems. Consequently, the design and operational requirements were for performance and safety, not cybersecurity. The "dumb" sensors and control systems that provided engineering data was useful only to the engineers. What changed was not the internet but the microprocessor. The microprocessor allowed for the calculation and conversion capability to take 1s and 0s that were not useful to anyone but that the engineers could convert to information that could be used by multiple organizations outside the engineering organization. It was the availability of this useful information that led to the desire to be able to share this information within and outside the immediate engineering facility. This enabled productivity improvements like "just-in-time" operation by sharing data with multiple organizations. The internet and modern networking technologies were the vehicles for disseminating this valuable information.

Modern communication technologies with improved analytics that are now employed at the smart device level enable Industry 4.0, the IIoT, transactive energy, and others, but at the price of significant cyber vulnerabilities that could affect the entire process. What is common among all these modern technologies that provide improved productivity is the dependence on reliable, accurate, and secure sensors, controls, and actuators. But what is missing? Cyber-secure sensors, controls, and actuators.

Figure 5 and Table 1 show some of the potential threat vectors to a control system environment. In some cases, the adversary is able to compromise the OT network from the IT environment. In other cases, the attacks come from physical attacks on the field network devices or software attacks injecting malware into the system during patches or firmware or software updates. There appears to be a lack of understanding about the number of potential attackers as well as the ease of attacking OT networks.



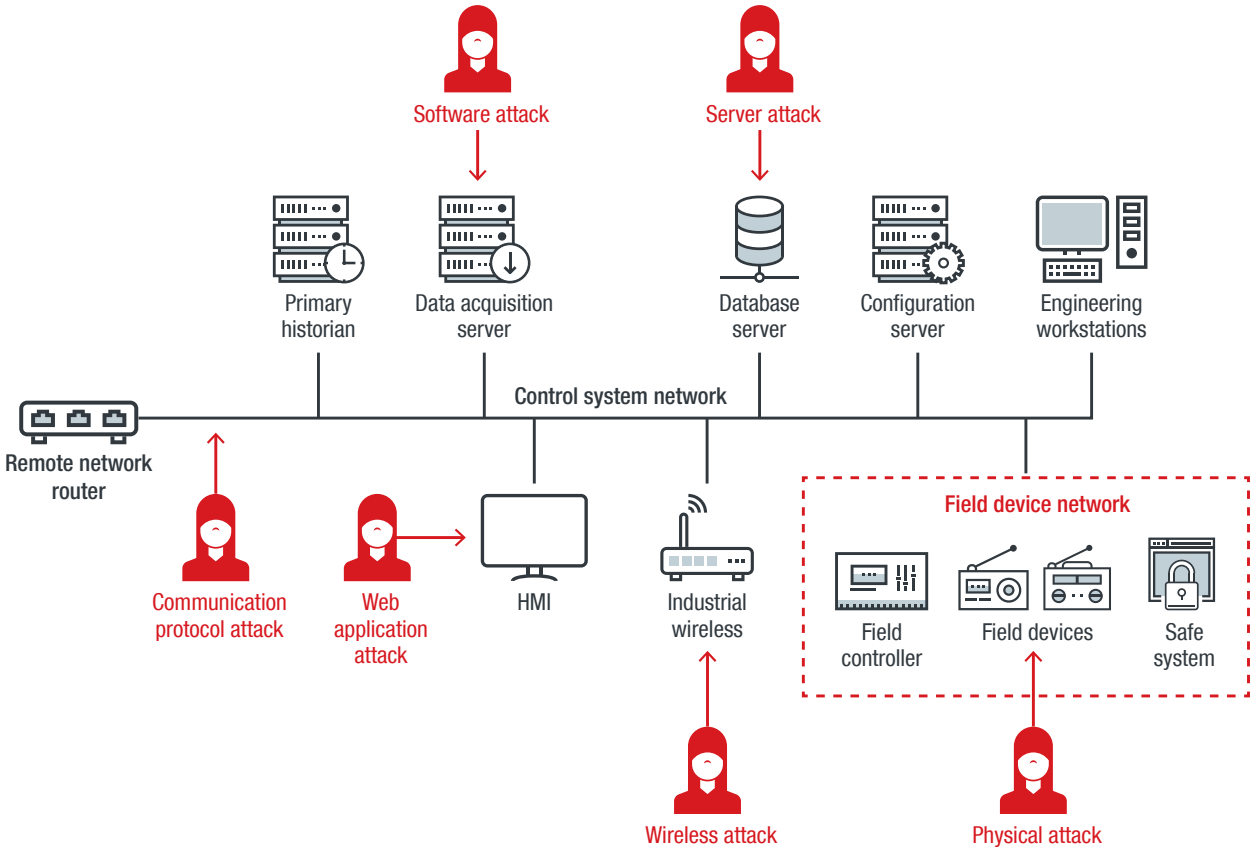


Figure 5. ICS attack vectors

Vector/Attack surface/Category	Security issue	Operational issue
Local area networks for collecting and locally processing data from connected ICS objects	Lack of authentication and security in process sensors	Compromised data could lead to equipment damage, regulatory issues, and personal safety hazards.
Transmission of data to the cloud via gateway	Lack of security protocols and gateways	
Processing and storage of data in the cloud by appropriate platforms and specific algorithms such as big data	Lack of data security	
Interfacing between platforms and end users for monitoring	Lack of secure communication protocols	Use of the cloud could lead to unforeseen operation concerns.
Device/Control system	Lack of security in the development life cycle, which introduces vulnerabilities and unsecure passwords	Compromised devices could lead to their use in botnet attacks or manipulation of equipment for performing harmful activities.

Table 1. Security challenges for OT environments

The Need to Address the Growing Gap Between IT/OT and Engineering

There has been a trend of highly integrated industrial automation sharing more constructs with IT (known as IT/OT convergence). As opposed to IT security, control system cybersecurity is still a developing area. Control system cybersecurity is an interdisciplinary field encompassing computer science, networking, public policy, and engineering control system theory and applications. Unfortunately, today's computer science curriculum often does not address the unique aspects of control systems, as shown in Figure 6. Correspondingly, electrical engineering, chemical engineering, mechanical engineering, nuclear engineering, and industrial engineering curricula do not address computer security. Consequently, there is a need to form joint interdisciplinary programs for control system cybersecurity both in the university setting and in the industry.[10] The cultural gap between the cybersecurity and engineering organizations is alive and well, and starts at the university level. The impact of this gap is felt in the disparity between the engineering systems and cybersecurity product designs, as they are diverging rather than converging.

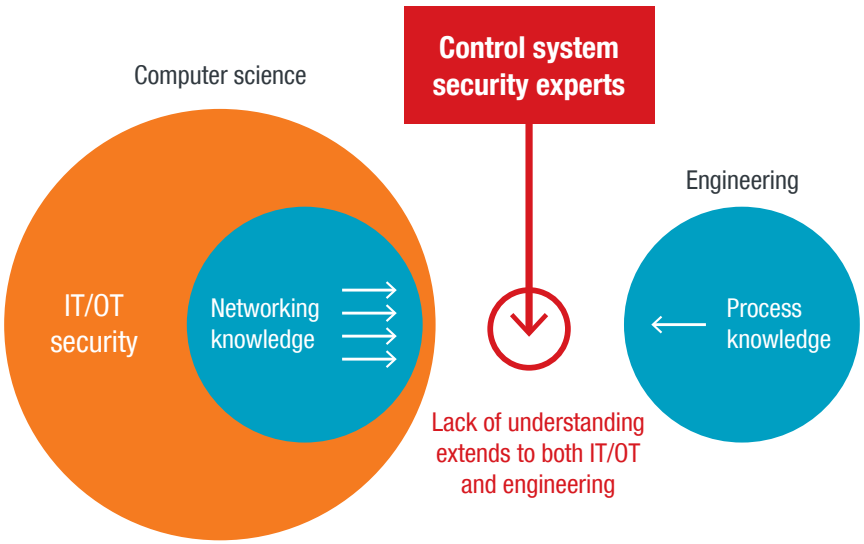


Figure 6. IT/OT vs. engineering – Packets vs. process

Misconceptions

The prevailing view is that control system information is not publicly available. There are a limited number of control system suppliers, which supply control systems to all industries globally. Control system information often includes common passwords that cross industries and continents. There are a limited number of major system integrators who also work on multiple industries worldwide. The control system vendor users' groups are open with multiple various information-sharing portals and other channels. Consequently, there is sharing of universal control system knowledge that is accessible by both defenders and attackers.

Another prevailing view is that network monitoring can detect all anomalies. However, it cannot detect communications from hardware backdoors. Some transformers have been known to include hardware backdoors, which allow attackers to remotely compromise the transformer control devices, including the load tap changer and protective relays, and consequently damage the transformers.

There is also a prevailing assumption that supervisory control and data acquisition (SCADA) systems or HMIs (master station) are used in all control systems. This is not true. For example, cruise control is a control system yet there is no operator display specific to cruise control — just on or off. Many people assume that SCADA is needed to keep lights on or water flowing. SCADA is for process optimization and view. There has been a US utility that had its SCADA system hacked and lost for 2 weeks, but there was no loss of power and therefore no disclosure to the authorities. Many people also assume that the operator can prevent damage by using the HMI. The HMI responds in many seconds to minutes. A compromise of a system can occur in milliseconds, which is too fast for any operator. This does not mean, however, that an organization does not need to secure its SCADA systems or HMIs. It still needs to do so because lack of visibility and control into these systems could result in operation downtime and costly business impact.

Many people assume that control system devices can be accessed only from Ethernet networks. This is also not true. In fact, this assumption is key to the Maginot Line, where all cybersecurity monitoring and mitigation assumes that all communications must go through the Ethernet networks. Monitoring the Ethernet networks is necessary, but it alone is not sufficient.

OT network security vendors and consultants assume the Level 0,1 process sensors or field devices are uncompromised, authenticated, and correct, and therefore the packet is all that needs to be monitored.

However, there is no cybersecurity, authentication, or cyberlogging at Level 0,1. Sensors have been demonstrated to drift, which is why they need to be recalibrated. Sensor configurations such as span, range, and damping cannot be monitored from the Ethernet networks, yet they can be compromised. The Corsair demonstrations from Moscow, Russia, at the ICS Cyber Security Conference in 2014 showed how Level 0,1 vulnerabilities could be exploited.[11]

Many people assume that network vulnerabilities correspond to physical system impact. They do not. It is generally not possible to correlate the severity of a network vulnerability with the potential for hardware impact. It is also not possible to correlate a network vulnerability with specific equipment such as pumps, motors, or protective relays. Consequently, the question is: What should engineers do when they are apprised of cyber vulnerabilities?

Many people equate cybersecurity to safety. They are related but not the same. A process can be cyber-secure but not safe, since there are other features besides cybersecurity that can make the process unsafe. Conversely, a process can be safe but not cyber-secure if devices that are independent of any network are used for process safety.

The gap between networking (whether IT or OT) and engineering is summarized in Table 2.

IT/OT (Networking)	Engineering
Zero trust	100% trust
Part of cybersecurity teams	Generally not part of any cybersecurity team
Worried about vulnerabilities	Worried about process and equipment
IP networks with security	Lower-level non-IP networks without security
Assume all comms go through IP network	Can get to Level 0,1 without IP network
Vulnerability assessments required	Level 0,1 not applicable
Nondeterministic	Deterministic
Worried about advanced persistent threats	Design features with no security
Focus on malicious attacks	Focus on reliability/safety

Table 2. Differences between networking and engineering

As can be seen in Table 2, networking and engineering are, in many cases, fundamentally different. Issues such as zero trust versus 100% trust fundamentally affect architecture, training, and policies. The difference between networking systems that are nondeterministic and control systems that are deterministic directly affects technology and testing. This difference has resulted in control systems having been shut down or even damaged because of the use of inappropriate network technology or testing tools.

Nature of ICS Cyberthreats

Because of the potential damage that cyberattacks could have on businesses, the economy, and the defense industry, control system cybersecurity should be a top-level national security concern and a priority for every business. However, this is not the case. Arguably the greatest hindrance to critical infrastructure cybersecurity is the refusal to acknowledge the problem. Neither the Solarium Commission Report nor the CyberMoonShot program, for example, addressed the unique issues with control systems.[12] And in an article titled "Dismissing Cyber Catastrophe," James Andrew Lewis, a senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS), says that a cyber catastrophe captures our imagination, but in the final analysis, it remains entirely imaginary and is of dubious value as a basis for policymaking. According to Lewis, there has never been a catastrophic cyberattack. These statements are obviously not true. Consequently, despite recent attempts to address the problem, public policy prescriptions, although helpful, are far from sufficient. In fact, articles such as Lewis' can dissuade organizations from focusing their attention on control system cybersecurity.[13]

ICS honeypots have demonstrated that control system networks and devices are being targeted. In 2013, Trend Micro published research on a honeypot for a water system that mimicked a real system, including an HMI and other components of an ICS environment. In that research, there were 12 targeted attacks out of 39 total attacks. From March to June 2013, Trend Micro 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.[14]

In 2015, Trend Micro released research around the Guardian AST monitoring system using a honeypot called GasPot, which simulated a gas tank monitoring system.[15] The purpose of this honeypot was to deploy multiple unique systems that did not look the same but nonetheless responded like real deployed systems. Trend Micro evolved the ICS honeypot by making it more and more realistic. The goal was to build a honeypot that appeared so real that not even a well-trained control system engineer would be able to tell that it was fake without diving deeply into the system.

First, Trend Micro decided on what services and ports would be exposed to the internet to make the honeypot attractive to attackers. At the same time, there were a minimal number of exposed services to prevent the honeypot from being identified as such. Second, Trend Micro created a backstory for the fictitious company, which included made-up employee names, working phone numbers, and email

addresses. The honeypot 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 control system markets around the world. Also, each PLC brand used a different protocol. Each PLC was loaded with logic and performed specific and associated tasks that together ran the manufacturing facility. These roles were agitator, burner control, conveyor belt control, and palletizer, which used a robotic arm. 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 and to simulate actual variations.

Not only are current attackers accustomed to encountering honeypots, but advanced actors also typically perform in-depth investigation — using open-source intelligence (OSINT), for example — before attacking a target system to make sure that they are not about to be "caught" by a honeypot system. For this reason, the honeypot did not only need 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, Trend Micro maintained the image of a real company and monitored the honeypot closely. The first attack we encountered came a month after the honeypot went live, with several others following in its wake. This showed that this sophisticated honeypot designed as a small business with critical clients and inadequate security was effective in luring threat actors.

During the May to December 2019 research period, it became apparent that there was increasing activity on the honeypot, with higher levels of interactions from day to day. However, the longer the honeypot was exposed, the greater the activity that we observed — and the more sophisticated attacks appeared to be compared to standard penetration-testing techniques.[16] This means that we created openings for attacks that could realistically be found in actual smart factories. This approach also demonstrated the need to have the different parties involved.

Cyberthreats and associated attacks are increasing, especially with more people working from home during the Covid-19 pandemic.[17] This is affecting both IT and OT networks. However, many control system designers and operators assume the cyber risk is only about email, which does not affect their job function, and therefore ignore or do not participate in cyber assessments. Consequently, the nature of control systems leads to a much higher risk than many people appreciate. Whereas the IT/OT communities operate under the premise of zero trust, the control system community operates under a 100% trust scenario, with many of the key organizations such as instrument engineers or technicians and safety system engineers or technicians not even part of many cybersecurity teams.

There is also another aspect particularly with certain government agencies. That is a reluctance to make control system cyber information available because of concerns that adversaries might learn from them. Unfortunately, this reluctance to share information affects the defenders as the offensive attackers make it a point to know the latest information.

The most probable control system cyberthreat is the unintentional impact that can come from either the control system engineers and technicians or the cybersecurity personnel. Often, a cyber incident from an insider is automatically tagged as an unintentional incident. This should not always be the case.

Another concern about malicious attacks is that they can be made to look like equipment malfunctions, as in what occurred with Stuxnet. Because there is limited ICS cyberforensics and training for control system engineers, most equipment malfunctions are not even investigated as possibly being cyber-related.

Culture and governance issues are critical to secure control systems. However, the governance model is such that cybersecurity is a network — not engineering — problem.[18] For control systems, this is a problem and this needs to change. The engineering organization is responsible for the control system equipment and understands how the control systems work and their system interactions. Many network security-induced control system cyber incidents have occurred because of lack of this knowledge.

In a new study, researchers demonstrate that weaponized disinformation campaigns could also hypothetically be exploited to execute relatively immediate attacks on critical infrastructures — using coercive methods to manipulate citizens into unwittingly wreaking havoc on the places they live.[19] Attackers are becoming better system engineers than defenders as they generally do not have organization charts, and the resultant silos, to meet. Often, sophisticated attackers work “backward” by determining what damage they want to cause and then look for tools to enable that to occur. For control systems, older network vulnerabilities are often sufficient to cause the desired impact, whereas defenders often focus on the latest network vulnerabilities without considering the physical impact that might or might not be created. Consequently, there is a need to understand and adapt to the myriad approaches attackers are using.

The culture gap has resulted in a focus on network forensics and training for IT/OT network security personnel. There is also a general willingness to share network attack details as the information becomes available. Unfortunately, cyberforensics does not exist for Level 0,1 devices, nor is there training for control system engineers. There has been a reluctance by governments to share actual control system cyber incidents. Control system and equipment vendors are often made aware of control system cyber incidents with their equipment but cannot share the information because of nondisclosure agreements. Consequently, there has been minimal identification or disclosure of actual control system cyber incidents.

The July 23, 2020, Alert AA20-205A, in which the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) recommend immediate actions to reduce exposure across operational technologies and control systems, states that control systems should not be connected directly to IT networks or the internet, or they will be compromised.[20] However, as of 2014, there had been more than 2 million control system devices directly connected to the internet.[21] Despite this and other warnings from authorities, there continues a push to connect control systems directly to the internet. The May/June 2015 issue of the ICS-CERT Monitor of the US Department of Homeland Security (DHS) specifically stated (sic): "If You're Connected, Your Likely Infected! Some asset owners may have missed the memo about disconnecting control system from the internet. Our recent experience in responding to organizations compromised during the BlackEnergy malware campaign continues to bring to light this major cybersecurity issue—Internet connected industrial control systems get compromised."[22]

Nature and History of Control System Cyber Incidents

Trend Micro has been tracking threats to ICS environments since the early 1990s. Figure 7 shows some of the most notable attacks on multiple organizations that we tracked from the past decade.

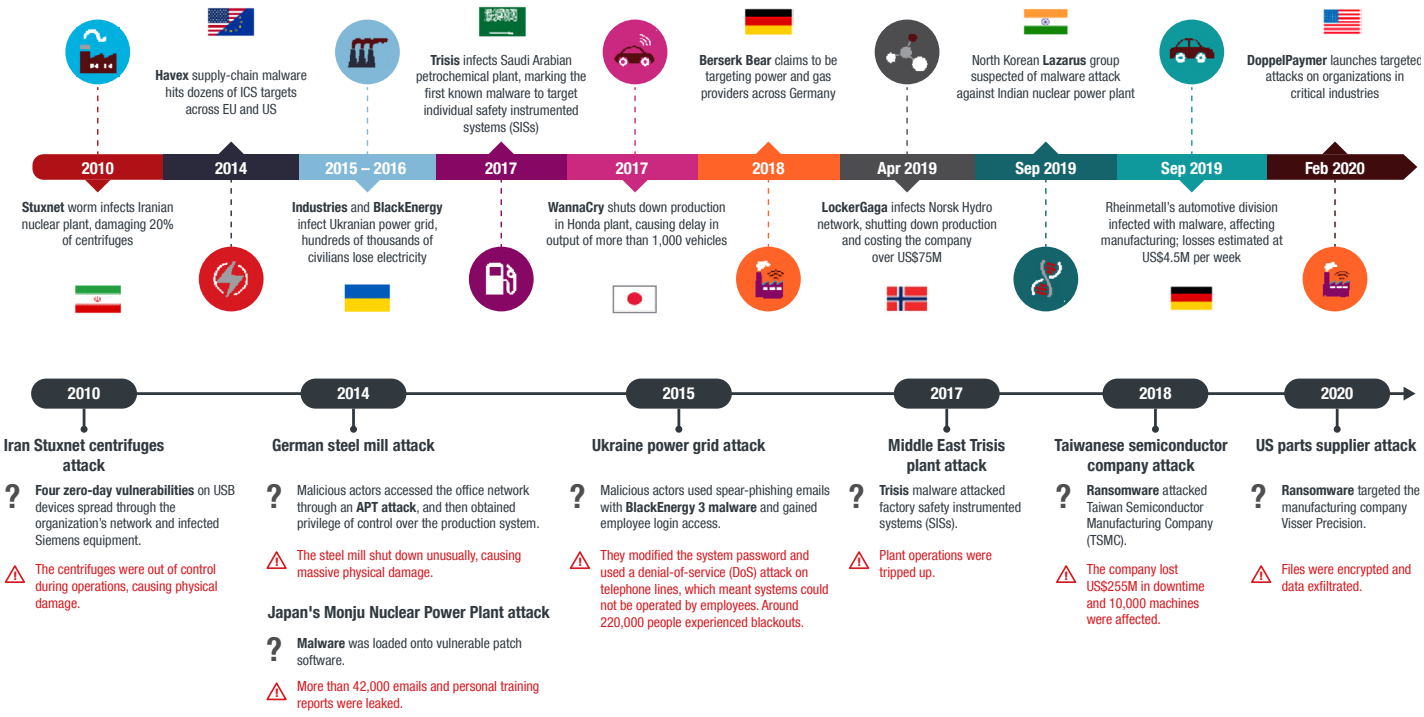


Figure 7. A timeline of industrial cyberattacks and their impact

Figure 8 shows a timeline of publicly identified cyberattacks on control system environments over the past couple of decades. The first nation-state ICS attack intended to cause physical damage occurred in 2010 with Stuxnet, which damaged approximately 20% of the centrifuges in an Iranian centrifuge facility. From the early virus attacks such as Blaster and Zotob, which caused denial of service (DoS) across multiple sectors, to the recent malware and intrusion attempts by hacking groups that have primarily caused operational downtime, the impact has resonated across multiple industries globally.

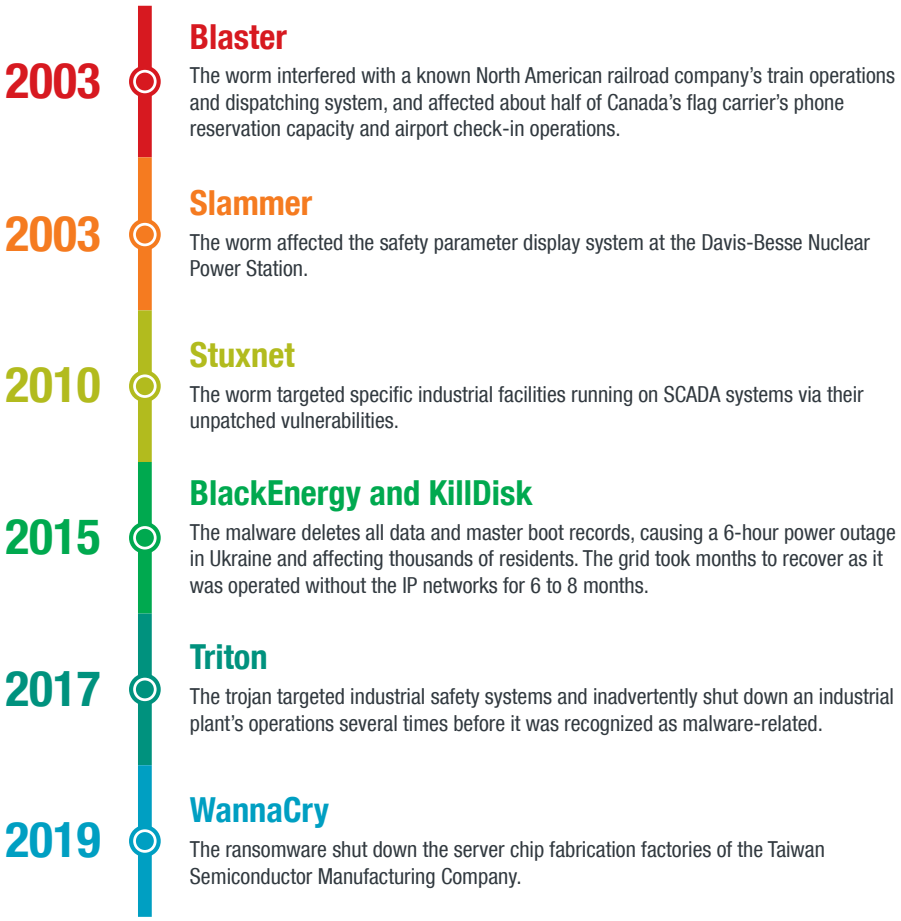


Figure 8. A timeline of publicly identified cyberattacks on control system environments

As of October 2020, Applied Control Solutions has amassed a database of almost 1,300 actual control system cyber incidents. Many of these cases are public, although the cyber aspects are not discussed. (The database is not public, but many were provided to us in confidence.) The cases are global in reach and include power (nuclear, fossil, hydroelectric, renewable), electric transmission and distribution, water/wastewater, pipelines, manufacturing, transportation, space, and defense. The impact ranges from trivial to significant environmental spills, significant equipment damage, and widespread blackouts. There have been more than 1,500 deaths and more than US$70 billion in direct damages to date. The focus of this database is control system cyber incidents that have had physical impact. Consequently, the database does not include the myriad network attacks and network vulnerabilities.

A team at Temple University in Philadelphia maintains a database of ransomware attacks on critical infrastructures.[23] According to the team's leader, Aunshul Rege, her team updates their dataset of critical infrastructure ransomware incidents (CIRWs) that have been publicly disclosed in the media or security reports. This CIRW dataset now has 747 records assembled from publicly disclosed incidents between 2013 and September 2020. These incidents were not counted in our database.

The first control system cyber incident occurred on Feb. 5, 1971. The Apollo 14 astronauts Alan Shepard and Edgar Mitchell were orbiting the moon and preparing to land on board their lunar module. A rogue bit of solder was floating around inside an emergency switch in the vehicle and shorting it out, thereby activating the abort button. In order to save the mission, Don Eyles, a computer engineer who worked on the computer systems in the lunar module, had to hack his own software. He came up with a few lines of instructions that he sent to the astronauts to lock out the emergency switch behavior. This enabled the Apollo 14 to land on the moon later that day.[24]

The first control system cyberattack occurred in February 1992 at the Ignalina Nuclear Power Plant in Lithuania, after which authorities arrested a computer programmer for attempting to sabotage the reactor with a computer virus.[25] The first control system cyber incident that resulted in fatalities was the Olympic Pipeline Company's gasoline pipeline rupture in June 1999. The first publicly known control system cyberattack was the Maroochy Shire wastewater incident in March 2000, where more than 750,000 liters of sewage were dumped on the grounds of a hotel. The first cyber-related physical attack was the March 2007 Aurora demonstration at the Idaho National Laboratory, where a diesel generator was destroyed by remotely opening and closing relays, causing the system to go into a "forbidden" operating zone. The first nation-state targeted cyberattack was Stuxnet in 2010. The first widespread control system cyberattack for economic reasons occurred in the Volkswagen cheat device case in 2015, which affected approximately 800,000 Volkswagen and Audi vehicles. Arguably the first case where a nation-state installed rogue hardware devices in control system equipment — it is unclear whether the June 1982 Siberian pipeline explosion was truly cyber or not — was the hardware backdoors installed in a large electric transformer in August 2019. This case resulted in the issuance of Presidential Executive Order 13920 in the US.[26]

One of the first significant cases where an unintentional cyber incident appeared to be a cyberattack was the penetration testing of protective relays in a large electric utility in 2017. In this case, the security group was scanning data center assets and then expanded the scanning into North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) substations, starting primarily at the 230/500 KV level. The security group had no previous experience with scanning substations. No notification was given for the scanning change to the internal support groups that are responsible for this function. The OT team was notified that substation scanning was started with a new security port scanning tool. Following the scans, the relays showed trouble, but the DNP (Distributed Network Protocol) polling was working properly and the networks in most substations were stable — SCADA was unaware of the problems. The port scanning of this new tool caused the real-time protocol operation of the relays (IEEE61850/GOOSE) to stop and suspend operation at the CPU (two different relay suppliers) and left the DNP/non-real-time operations alone — the worst possible circumstance.

To clear the trouble and restore operation, each relay had to be cut out and rebooted. Several hundred relays were affected. All the devices in each substation were affected at the same time in every case.

Without knowing that a security scan was initiated, it looked like a distributed denial-of-service (DDoS) attack resulting in equipment malfunction. IEC 61850 was one of the protocols affected. Additionally, a unique port scanner was used, which had the effect of a DoS disruption of relays that had to be manually reset.

According to ESET's report on Industroyer, the attackers' arsenal included a port scanner that could be used to map the network and to find computers relevant to their attack. Instead of using existing software, the attackers built their own custom-made port scanner. The attackers could define a range of IP addresses and a range of network ports to be scanned by this tool. Another tool from the attackers' arsenal was a DoS tool that exploited the CVE-2015-5374 vulnerability to render a device unresponsive. (This vulnerability disclosure was for one specific vendor's relays, and the question is how vulnerable it would be to other vendor's relays). Once this vulnerability is successfully exploited, the target device would stop responding to any commands until it would be rebooted manually. To exploit this vulnerability, the attackers hard-coded the device IP addresses into this tool. Once the tool is executed, it would send specifically crafted packets to port 50,000 of the target IP addresses using UDP (User Datagram Protocol). Because the impact at this utility was very similar to that of the Industroyer malware, this utility event could have been mistaken as a "test" run of the Industroyer malware.

The similarities between the impact at this utility and that of the Industroyer report raise these questions:

- Was this event totally coincidental to the impact of Industroyer? If so, what other unintentional incidents can cause equipment problems and be indistinguishable from cyberattacks?
- Was the Industroyer malware somehow loaded onto the penetration tester's software because the attackers knew the utility's substation configuration? If so, why did the utility's cybersecurity program not detect the malware particularly after being informed of Industroyer? Is the malware still resident? How many other utilities would be incapable of detecting this malware?
- Did the developers of Industroyer know that "innocent" penetration-testing software could cause this kind of impact? If so, was the Industroyer malware developed to mimic the unintentional impact, making the malware detection very difficult at best?
- How many other software products that could cause grid disruptions have been mimicked?

These cases lead to the inability to clearly distinguish between unintentional impact and a cyberattack, making it difficult at best to meet NERC CIP and NEI-0809 malware identification requirements. These cases also make it clear that before using new penetration-testing software, there is a need to test existing relays offline prior to using penetration-testing software in a live condition.

The February 2017 report of the Office of Inspector General of the National Aeronautics and Space Administration (NASA)[27] provided these three case histories where IT technologies had impact on control systems and operations, demonstrating the need for engineering and cybersecurity "convergence":

- A large-scale engineering oven that uses OT 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 could be exploited by an attacker caused failure of equipment 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.

Cybersecurity Strategy and Security Controls

Reducing cyber risk in an ICS environment requires significant understanding of a network environment, including the sensors, the process controls, the protocols, and the communications across each level of the Purdue Reference Model (as shown in Figure 2) as well as the threats to and the vectors in the environment. The cyber risk affects all types of industries — power, oil and gas, manufacturing, pharmaceutical, healthcare, and transportation, among others — and it is recommended that every organization implement a cybersecurity strategy.

Implementing cybersecurity in industrial controls and critical infrastructure environments is critical because the wrong strategy and security controls can cause significant operation downtime or create safety issues. The reasons are:

- Many organizations, especially on the ICS side, have a shortage of domain knowledge and expertise.
- There is uncertainty as to the roles and responsibilities or governance across the organization.
- It is difficult to improve the return on investment (ROI).
- Some organizations tend to put the economic considerations or profitability of the company over cybersecurity.

In addition to these business challenges, there are technical challenges to overcome. These include:

- Unknown devices and connections to the OT network (shadow OT).
- Lack of security in the original design.
- Vulnerable and unsecure third-party applications and operating systems.
- Legacy systems and environments that have been around for many decades and that may not be able to be secured.

Recommendations

To ensure the effectivity of a cybersecurity strategy, there must be a cohesive interaction among its four pillars: people, process, technology, and culture.[28]

People: No matter the industry it is in, any organization needs to develop appropriate training on cybersecurity and other people skills as there is a need for integration throughout the organization. It also needs to formulate guidelines and lay out a plan that clearly outlines the collaboration between IT and OT teams, further strengthening the human factor. According to over 62% of the respondents in a 2019 SANS survey on the state of OT/ICS cybersecurity,[29] the human factor was considered the greatest security risk to their operations, but most organizations' security budgets for it were less than US$100,000 in 2019. This needs to change: Since a trained and security-aware organization can reduce security risk significantly, people should be the starting point of any organization's cybersecurity strategy investment.

Process: For a cybersecurity strategy to be successful, an organization must develop and implement procedures while ensuring that clear roles, responsibilities, and management systems are put in place. In addition, the process needs to include a governance, policy, and best practice framework, and it must be periodically tested to evaluate and ensure its efficacy. If the process is forgotten or broken, it could lead to cyber risk. The 2019 SANS survey left much to be desired in this regard: It found that only 14% of the respondents considered the process as the greatest security risk, and nearly half of organizations' budget allocation for it did not exceed US$500,000 in 2019.

Technology: The lack of understanding of appropriate OT deployment has led to many control system cyber incidents resulting in downtime or even creating safety challenges for organizations. For example, deploying an IT vulnerability scanner in an OT environment can cause process control system shutdowns because of incompatibility of protocols, the types of applications running, or operating systems. Cybersecurity stakeholders across the executive, IT, and OT segments of an organization should therefore ensure the proper testing, integration, and use of technology in the IT/OT environment. In the 2019 SANS study, only 22% of the respondents considered technology deployment as the greatest security risk, yet most organizations did not invest sufficiently in OT/ICS security compared to their IT budget, which exceeded US$1 million in the case of more than 40% of them.

Culture: The 2019 SANS survey found that around 84% of organizations had already adopted or were planning to adopt an IT/OT convergence cybersecurity strategy. But for any such strategy to be effective, a cyber culture, which is essential to the reduction of cyber risk, must be developed and implemented within an organization. The fostering of this culture must start from the top and be communicated down to all levels of the organization. For the OT environment, this includes the engineering and operational organizations responsible for the equipment that is being secured.

Figure 9 summarizes the key components of the four pillars of an effective cybersecurity strategy.

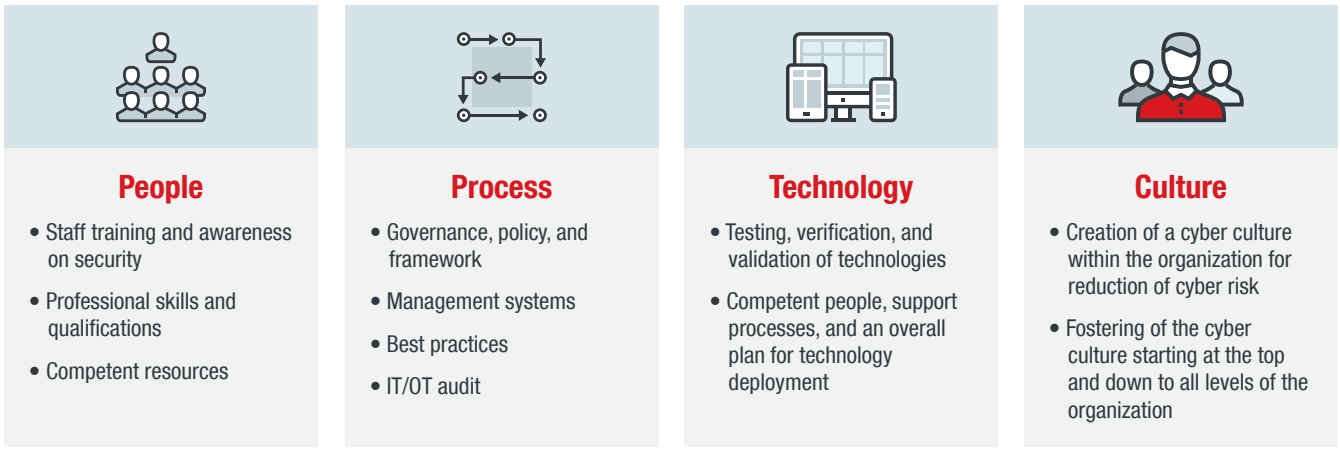


Figure 9. The four pillars of an effective cybersecurity strategy

A good place to start in developing and implementing a successful cybersecurity strategy is with industry standards that your organization needs to align with. Depending on your industry, you will need to look at standards that can be applied to your business or vertical. Industry standards, examples of which are indicated in Figure 10, can provide best practices for protecting ICSs.

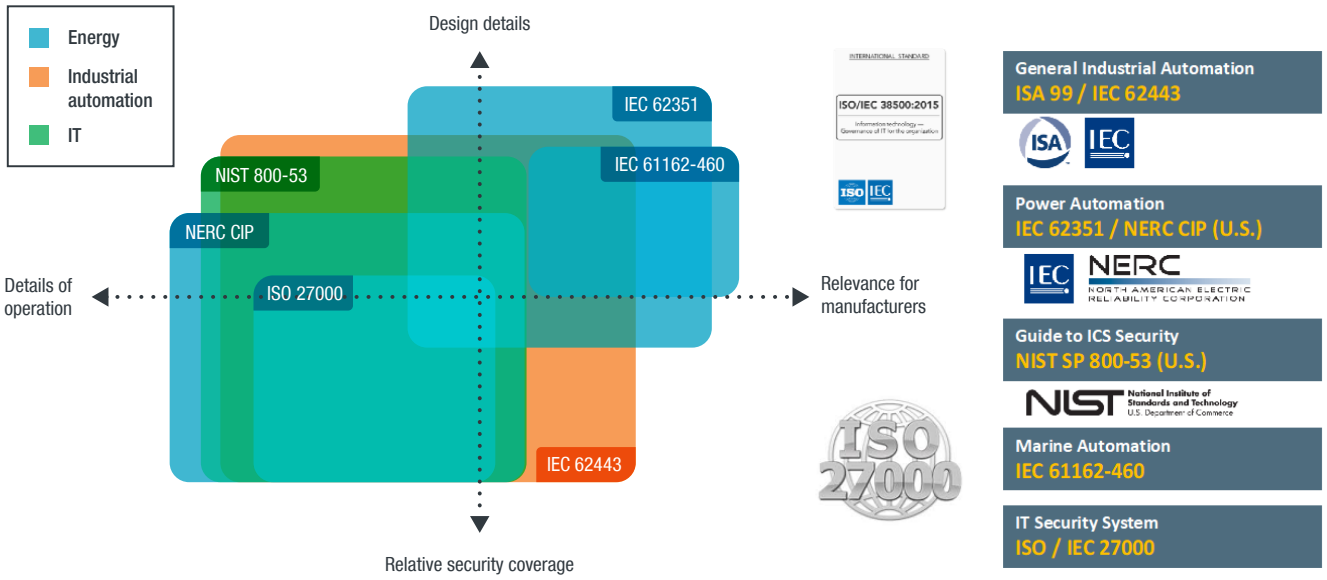


Figure 10. Examples of industry standards

Next, develop a cybersecurity framework that can be appropriately applied to your organization's goals and objectives. Ensure you have the right people, process, technology, and culture to deal with different cyber incidents and be able to recover quickly to ensure business continuity. At the same time, ensure that cyber incidents will not happen again in the future, or if they do happen again, they will have minimal impact on the business and its operation.

Figure 11 shows a high-level example of a cybersecurity framework, illustrating the process that an organization needs to go through in the event of a cyberattack. Figure 12 shows a high-level example of a network architecture in a large enterprise, including both IT and OT environments and the different cybersecurity technologies that could be applied as well as the risks and threats that could affect the environment.

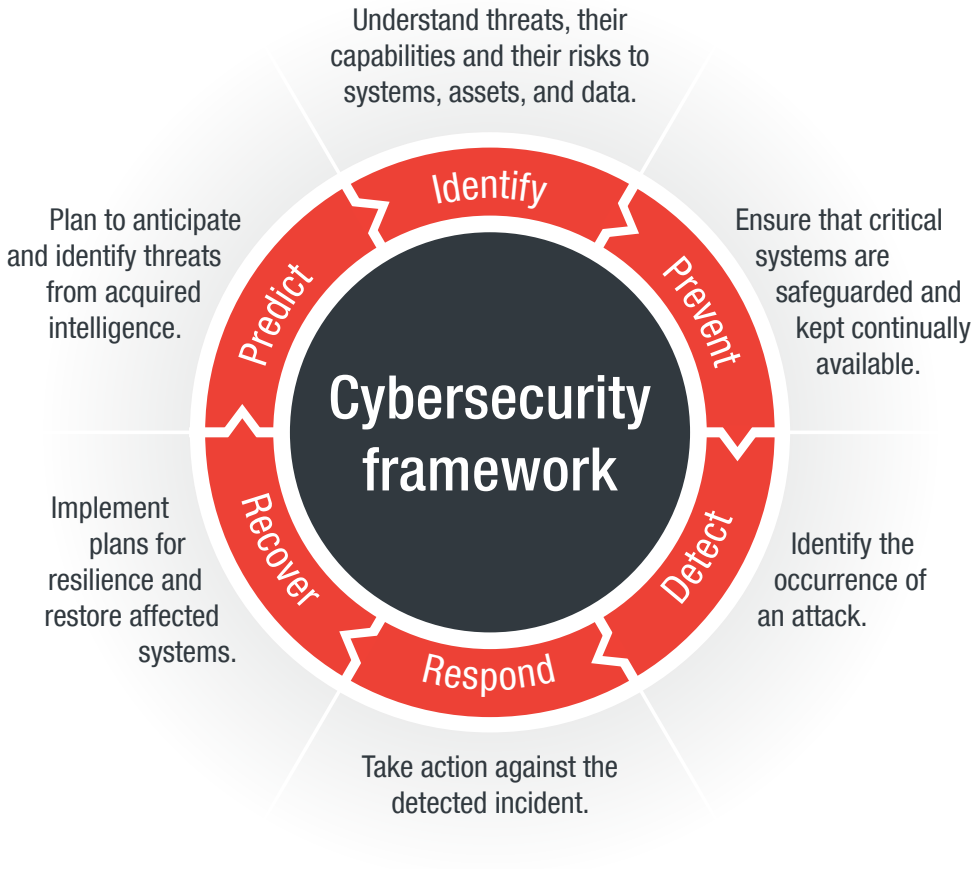


Figure 11. A high-level example of a cybersecurity framework

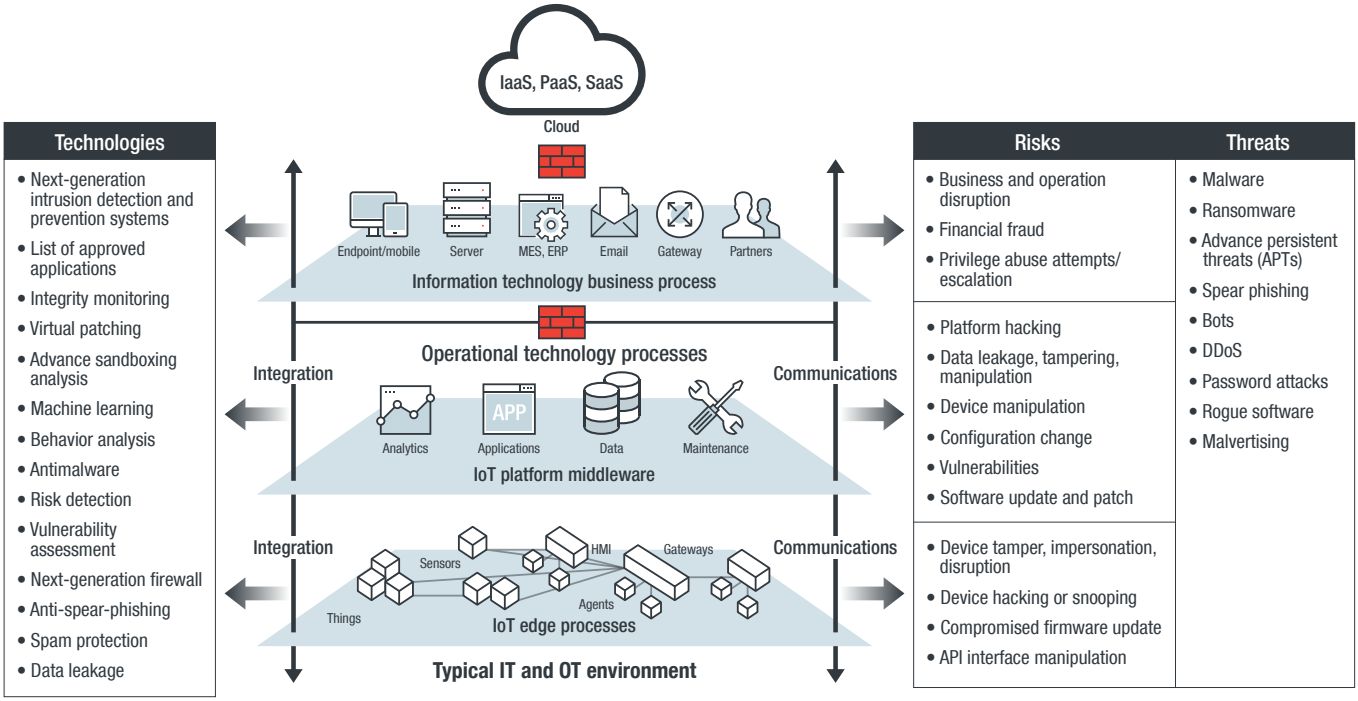


Figure 12. A high-level example of a network architecture in a large enterprise

Everyone knows about cybersecurity. The challenge is knowing how to apply it with the right capabilities and technologies. Table 3 provides some guidelines as to what an organization will need.

Visibility on assets, protocols, control commands, and threats	Real-time protection and enforcement to prevent security breaches with minimum overhead	Security of the OT/ICS network to keep the operation running, reliable, and safe
Comprehensive protection at the network, endpoint, server, cloud, and virtualization environments	Adaptive solution to fit into existing IT/OT infrastructure and operation	Centralized management for distributed, multitier deployments and integration with SIEM/SOAR platforms

Table 3. Guidelines for purpose-built OT/ICS security solutions

Implementing cybersecurity baseline security controls does not have to be expensive for the organization. The following are some basic activities that your organization can carry out to reduce cyber risk and make it more difficult for adversaries to succeed in their attacks, if the network is compromised:

- Strengthen account credentials, particularly passwords.
- Disable unused physical and network service ports.
- Encrypt the system configuration file.
- Allow only permitted IP and media access control (MAC) addresses to access the network.
- Use secure or encrypted communication protocols in the IT/OT/ICS environment.

- Back up all system configurations regularly so that systems can be restored in case of compromise.
- Implement cybersecurity education and training for all levels of employees in the organization, including performing regular phishing-attack scenarios across the employee population.
- Perform random security checks and audits across your organization to ensure that cybersecurity policies are being followed.
- Ensure visibility and perform asset management of all devices across IT and OT environments, including contractor devices, newly acquired devices, and any transient or air-gap devices.

Figure 13 shows a high-level enterprise architecture that is mapped to the ISA/IEC 62443 reference model. It shows how to implement a defense-in-depth cybersecurity strategy across OT/ICS, IT, air-gap, and cloud environments. On the left side is the OT network, on the right side is the traditional IT network, and at the top are the cloud or edge and some transient or air-gap devices or contractor devices. Depending on the maturity of the organization's digital transformation or cybersecurity strategy, these networks could be converged into one or they may be separate. For this example, these networks are assumed to be already converged.

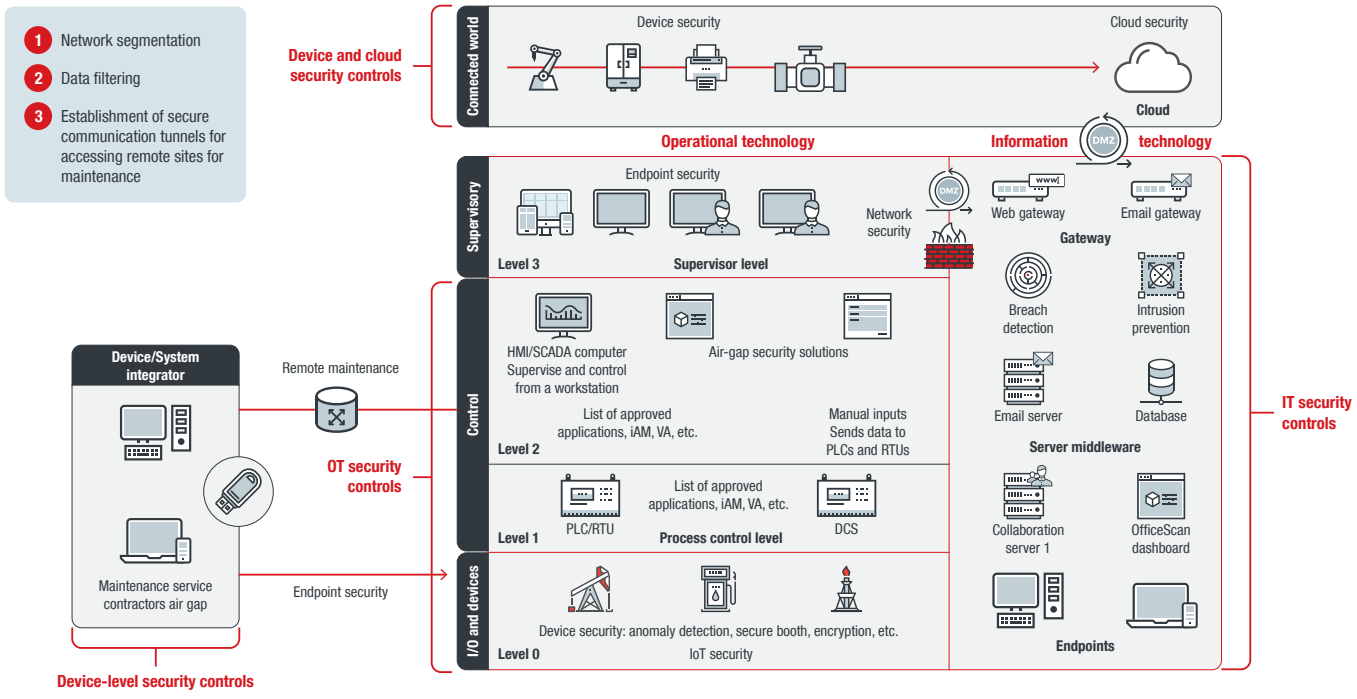


Figure 13. Defense-in-depth protection for ICSs

Defense-in-depth protection for ICSs need to include the following key components:

- Holistic approach: secure development life cycle, threat intelligence, incident response, cybersecurity strategy (people, process, technology, culture)
- SaaS, cloud, virtualization, and container security: firewall, intrusion prevention system (IPS), antivirus, integrity monitoring, data loss prevention (DLP), allow list, configuration management
- Security visibility, monitoring, and management: IT/OT, cloud/virtualization, and SaaS; integration with SIEM/SOAR platform
- Network infrastructure security: micro segmentation, virtual patching, allow list, antivirus, sandboxing, firewall, intrusion prevention/detection system (IPS/IDS), DLP, encryption, zero trust
- Device and endpoint security: antivirus, allow list, DLP, integrity checking, virtual patching, vulnerability assessment scanning
- Transient, air-gap environment security: antivirus, allow list, DLP, integrity monitoring

Summary

Governance should be modified to include all affected organizations in cybersecurity. This would include operations, maintenance, cyber and physical security, forensics, business continuity, procurement, communications, and others as necessary. This would also include engineering management as part of cyber policymaking. Sensitivity training should be provided to the various organizations to ensure that they understand the impact that security policies or technologies could have on engineering systems.

Control system cybersecurity policies should be developed based on actual incidents. Other policies such as IT security policies, physical security policies, and business continuity policies should be such that they do not impact control systems.

All network tools for use with control systems should have been adequately tested offline before they are employed in real-time OT networks.

For the OT/ICS environment, the appropriate technologies should be used, accordingly tested first in an integrated manner offline, then online. These technologies include the suite of OT cybersecurity technologies developed by Trend Micro and TxOne Networks.[30]

References

1 The White House, Washington. (May 22, 1998). *Federation of American Scientists*. "Presidential Decision Directive/NSC-63." Accessed on Dec. 4, 2020, at https://fas.org/irp/offdocs/pdd/pdd-63.htm.

2 FieldComm Group. (n.d.). *FieldComm Group*. "HART Technology." Accessed on Dec. 4, 2020, at www.fieldcommgroup.org.

3 Profibus. (n.d.). *Profibus*. "Profibus." Accessed on Dec. 4, 2020, at https://www.profibus.com.

4 Fieldbus Foundation. (n.d.). *Fieldbus Foundation*. "Fieldbus." Accessed on Dec. 3, 2020, at http://www.fieldbus.org.

5 Gartner. (n.d.). *Gartner*. "Operational Technology (OT)." Accessed on Dec. 4, 2020, at https://www.gartner.com/en/information-technology/glossary/operational-technology-ot.

6 National Institute of Standards and Technology. (March 2006). *NIST*. "Minimum Security Requirements for Federal Information and Information Systems." Accessed on Dec. 4, 2020, at https://csrc.nist.gov/publications/detail/fips/200/final.

7 International Society of Automation. (n.d.). *ISA*. "ISA99, Industrial Automation and Control Systems Security." Accessed on Dec. 4, 2020 at https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99.

8 Pascal Ackerman. (October 2017). *Packt*. "Industrial Cybersecurity." Accessed on Dec. 4, 2020, at https://subscription.packtpub.com/book/networking_and_servers/9781788395151.

9 Keith Shaw. (Oct. 14, 2020). *Network World*. "The OSI model explained and how to easily remember its 7 layers." Accessed on Dec. 4, 2020, at https://www.networkworld.com/article/3239677/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html.

10 Joseph Weiss. (2010). *WorldComp 2010, Las Vegas, Nevada*. "The Need for Interdisciplinary Programs for Cyber Security of Industrial Control Systems."

11 Joe Weiss. (Oct. 27, 2014). *Control Global*. "Highlights from the 2014 ICS Cyber Security Conference." Accessed on Dec. 4, 2020, at https://www.controlglobal.com/blogs/unfettered/highlights-from-the-2014-ics-cyber-security-conference/.

12 Joe Weiss. (March 23, 2020). *Control Global*. "The Solarium Commission report and its incomplete applicability to control systems and critical infrastructure." Accessed on Dec. 4, 2020, at https://www.controlglobal.com/blogs/unfettered/the-solarium-commission-report-and-its-incomplete-applicability-to-control-systems-and-critical-infrastructure/.

13 Joe Weiss. (Aug. 31, 2020). *Control Global*. "A critical look at the CSIS Report "Dismissing Cyber Catastrophe."" Accessed on Dec. 4, 2020, at https://www.controlglobal.com/blogs/unfettered/a-critical-look-at-the-csis-report-dismissing-cyber-catastrophe.

14 Kyle Wilhoit. (2013). *Trend Micro*. "The SCADA That Didn't Cry Wolf: Who's Really Attacking Your ICS Equipment? (Part 2)." Accessed on Dec. 4, 2020, at https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-scada-that-didnt-cry-wolf.pdf.

15 Trend Micro. (Aug. 6, 2015). *Trend Micro*. "The Gaspot Experiment: How Gas-Tank-Monitoring Systems Could Make Perfect Targets for Attackers." Accessed on Dec. 4, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-gaspot-experiment.

16 Trend Micro. (Jan. 21, 2020). *Trend Micro*. "Fake Company, Real Threats: Logs From a Smart Factory Honeypot." Accessed on Dec. 4, 2020, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot.

17 Trend Micro. (Nov. 11, 2020). *Trend Micro*. "Developing Story: COVID-19 Used in Malicious Campaigns." Accessed on Dec. 4, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

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

19 Peter Dockrill. (Aug. 22, 2020). *Science Alert*. "Weaponised Disinformation Could Unleash City-Wide Blackouts, Researchers Warn." Accessed on Dec. 4, 2020, at https://www.sciencealert.com/weaponised-disinformation-could-unleash-city-wide-blackouts-scientists-warn.

20 CISA. (July 23, 2020). *CISA*. "Alert (AA20-205A): NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems." Accessed on Dec. 4, 2020, at https://us-cert.cisa.gov/ncas/alerts/aa20-205a.

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

22 ICS-CERT Monitor. (May/June 2015). *ICS-CERT Monitor*. "ICS-CERT Monitor." Accessed on Dec. 4, 2020, at https://us-cert.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf.

23 Eduard Kovacs. (Sept. 12, 2020). *SecurityWeek*. "University Project Tracks Ransomware Attacks on Critical Infrastructure." Accessed on Dec. 4, 2020, at https://www.securityweek.com/university-project-tracks-ransomware-attacks-critical-infrastructure.

24 Stephen Cass and Christina Dabney. (July 10, 2018). *IEEE Spectrum*. "Don Eyles: Space Hacker." Accessed on Dec. 4, 2020, at https://spectrum.ieee.org/video/aerospace/space-flight/don-eyles-space-hacker.

25 William C. Potter. (Aug. 20, 1997). *NTI*. "Less Well Known Cases of Nuclear Terrorism and Nuclear Diversion in Russia." Accessed on Dec. 4, 2020, at https://www.nti.org/analysis/articles/less-well-known-cases-nuclear-terrorism-and-nuclear-diversion-russia/.

26 Office of Electricity. (Nov. 1, 2020). *Department of Energy*. "Securing the United States Bulk-Power System Executive Order." Accessed on Dec. 4, 2020, at https://www.energy.gov/oe/bulkpowersystemexecutiveorder.

27 NASA Office of Inspector General, Office of Audits. (Feb. 8, 2017). *NASA*. "Industrial Control System Security Within NASA's Critical and Supporting Infrastructure." Accessed on Dec. 4, 2020, at https://oig.nasa.gov/docs/IG-17-011.pdf.

28 Damiano Bolzoni. (July 11, 2019). *Forescout*. "3 Pillars for a Successful IT-OT Cybersecurity Strategy: People, Process & Technology." Accessed on Dec. 9, 2020, at https://www.forescout.com/company/blog/3-pillars-for-successful-it-ot-cybersecurity-strategy/.

29 Forescout. (2019). *Forescout*. "The 2019 SANS State of OT/ICS Cybersecurity Survey." Accessed on Dec. 9, 2020, at https://www.forescout.com/platform/operational-technology/2019-sans-state-of-ot-ics-cybersecurity-survey/.

30 Trend Micro. (n.d.). *Trend Micro*. "Smart Factory Security." Accessed on Dec. 4, 2020, at https://www.trendmicro.com/en_us/business/solutions/iot/smart-factory.html.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research