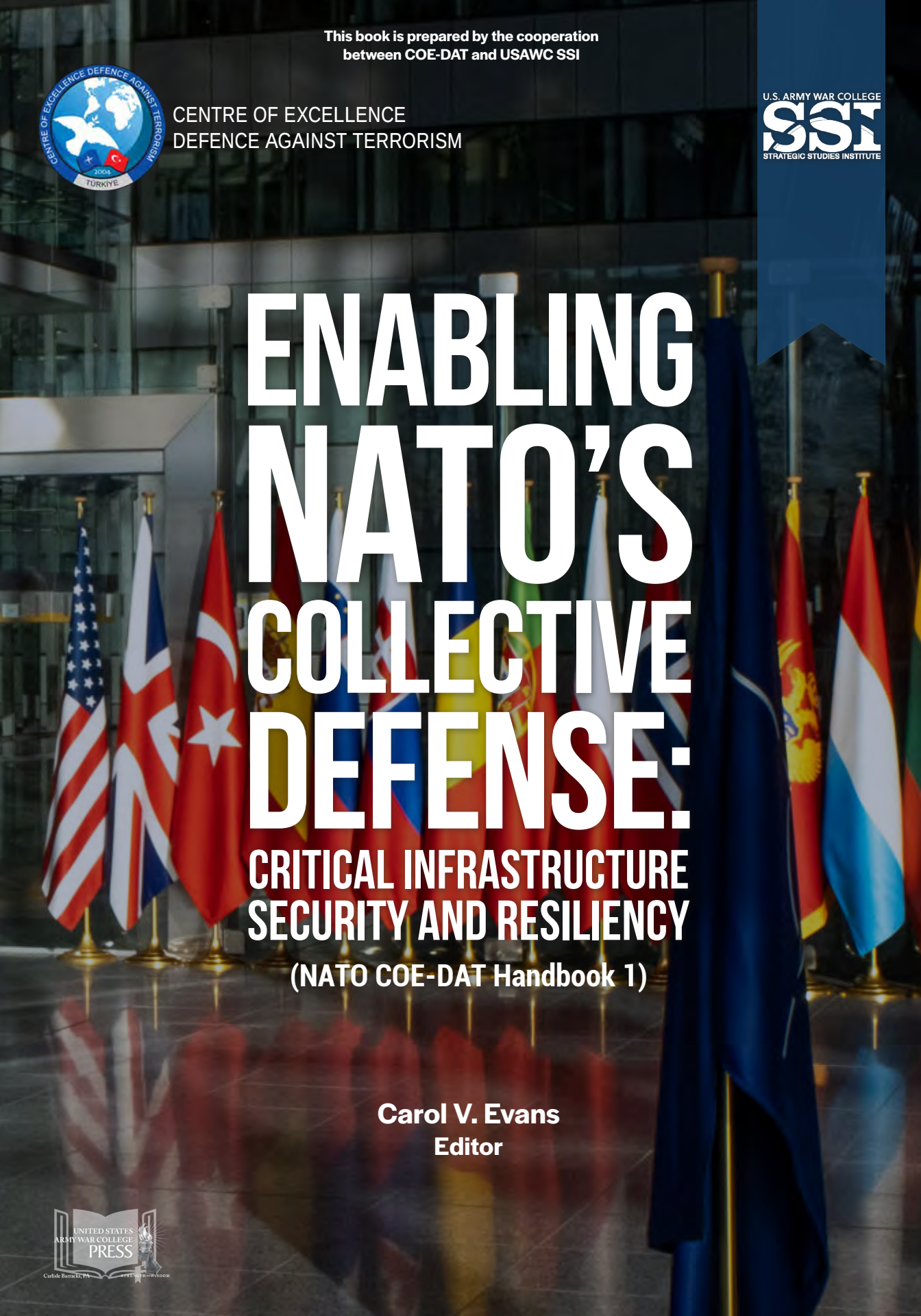

This book is prepared by the cooperation between COE-DAT and USAWC SSI

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM

U.S. ARMY WAR COLLEGE SSI STRATEGIC STUDIES INSTITUTE

ENABLING NATO'S COLLECTIVE DEFENSE:

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCY

(NATO COE-DAT Handbook 1)

Carol V. Evans
Editor

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA

This paper is excerpted from "Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)" published by Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press (ISBN: 1-58487-840-1) on 15 November 2022, available at https://press.armywarcollege.edu/monographs/955/.

— 14 —

Enhancing Cybersecurity of Industrial Control Systems

Sungbaek Cho

Due to the advancement of information and communications technologies, most modern critical infrastructure operates electronically. Malevolent forces could exploit any weaknesses or vulnerabilities in the devices and equipment that comprise these critical infrastructure systems to launch cyberattacks that adversely affect the society and its national security. For instance, cyber incidents targeting lifeline sectors—such as electricity, water supply, and transportation—may not simply lead to inconvenience and financial losses for people and businesses, they can also cause social turmoil, disruption of military operations, and human casualties or fatalities. For these reasons, most countries regard the cyber defense of critical infrastructure systems and assets as a top priority, and they are undertaking extensive efforts to enhance their critical infrastructure security and resilience (CISR) posture.

The North Atlantic Treaty Organization identifies cyberattacks against critical infrastructure as a possible instability situation, defined as a future event significant enough to reach the threshold requiring the Alliance to use military forces.[1] As national and societal functions rely heavily on information technology, improving cybersecurity has become a significant element of member states' efforts to enhance national CISR. Similarly, NATO has identified the important link between cybersecurity and the Alliance's

1. NATO, *Framework for Future Alliance Operations: 2018 Report* (Norfolk, VA: Allied Command Transformation, 2018), 15, https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf.

ability to fulfill its core tasks. At the Warsaw Summit in 2016, NATO officially recognized cyberspace as a domain of operations in which the Alliance must "defend itself as effectively as it does in the air, on land, and at sea."[2] At Warsaw, the Allies also pledged to strengthen and enhance the cyber defenses of national networks and critical infrastructure as a matter of priority, highlighting that NATO as an organization is only as strong as its weakest link.[3] NATO now serves as a venue in which Allies can consult on cyber defense issues, share information on cyber threats, exchange best practices, and coordinate activities including education, training, and exercises.[4]

Depending on its scale and severity, a cyberattack against a NATO member state's critical infrastructure could be regarded in the same way as an armed attack that would justify the targeted country's right to self-defense.[5] A destructive cyberattack also could lead Allies to invoke Article 5 of the Washington Treaty—the mutual defense clause that states an attack against one Ally is an attack against all Allies—though such a decision would be taken by the North Atlantic Council on a case-by-case basis.[6] In response to the evolving cyber threat landscape, NATO's stance against cyberattacks was further extended at the Brussels Summit in 2021, where Allied leaders recognized that the impact of cumulative, malicious cyber activities could amount to an armed attack.[7] The term *cumulative* implies several lower-impact cyberattacks by the same adversary over time could be as destructive as a single, massive cyberattack.[8] Regarding cyber operations against adversaries, NATO doctrine introduces a concept known as Sovereign Cyber Effects Provided Voluntarily by Allies, a mechanism that allows individual member states to support voluntarily other Allies' offensive cyber capabilities in the case of armed

2. "Warsaw Summit Communiqué," NATO (website), July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

3. "Cyber Defence Pledge," NATO (website), July 8, 2016, https://www.nato.int/cps/su/natohq/official_texts_133177.htm.

4. "Fact Sheet: NATO Cyber Defence," NATO (website), August 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/8/pdf/2008-factsheet-cyber-defence-en.pdf.

5. Michael N. Schmitt, general ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* 2nd ed., managing ed. Liis Vihul (Cambridge, UK: Cambridge University Press, 2017), 339–48.

6. "Wales Summit Declaration," NATO (website), September 5, 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

7. "Brussels Summit Communiqué," NATO (website), June 24, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

8. Stefan Soesanto, "When Does a 'Cyber Attack' Demand Retaliation? NATO Broadens Its View," Defense One (website), June 30, 2021, https://www.defenseone.com/ideas/2021/06/when-does-cyber-attack-demand-retaliation-nato-broadens-its-view/175028/.

conflicts, and outlines the procedures for defensive cyber operations, including self-defense and collective defense.[9]

Although NATO is taking steps to improve its collective ability to defend against and respond to cyberattacks against Allied critical infrastructure, it should be kept in mind that individual member states form the first line of defense. Thus, enhancing cyber defense capabilities and enhancing CISR policies and procedures are the primary responsibilities of each Ally. With these objectives in mind, this chapter aims to provide an overview of the major cybersecurity issues surrounding critical infrastructure with a special focus on industrial control systems (ICS). Based on this understanding, the chapter will offer best practices and tools for critical infrastructure stakeholders, owners, and operators to protect their systems and enhance security and resilience against cyberattacks.

An Overview of Industrial Control Systems (ICS)

To understand cybersecurity requires a proper knowledge of ICS. The term ICS includes various control systems typically found in industrial sectors and critical infrastructure. Also known as operational technology (OT), an ICS consists of combinations of different control components (electrical, mechanical, hydraulic, and pneumatic, for instance) to achieve an industrial objective, such as manufacturing, transportation, or energy.[10] Examples of ICS include power plants, electrical grids, water and water treatment systems, energy transport, and railways. While an ICS can be configured and operated in a variety of ways, there are three common control systems that merit further explanation.[11]

- Supervisory control and data acquisition (SCADA) systems are used to control dispersed assets centrally. Typical examples are water distribution, wastewater collection, power grids, railways, and other public transportation systems.

9. NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations,* Allied Joint Publication 3.20 (Brussels: NATO, 2020), 5, https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320.

10. National Institute of Standards and Technology (NIST), *Guide to Industrial Control Systems (ICS) Security* (Washington, DC: Department of Commerce, 2015), B-8, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

11. NIST, *Industrial Control Systems*, 2-5–2-13.

- Distributed control systems (DCS) manage continuous production processes within the same geographic area. Examples include oil refineries, water and wastewater treatment facilities, power plants, chemical plants, and pharmaceutical processing facilities.
- Programmable logic controllers (PLC) are devices that control discrete processes, such as automobile assembly lines. While a PLC is often used as a component for a SCADA system or DCS, it can also be implemented as the primary controller in a small ICS.

While actual ICS architectures vary widely based on the nature of the critical infrastructure sector and type of facility, the Purdue reference architecture is widely recognized as the standard model for common control systems.[12] Having a model that depicts the control system architecture and shows the various interconnections between technological components can help organizations segment the various networks, develop zones with clear boundaries, and create layers of cyber defense measures. The US Department of Homeland Security (DHS) recommends this process of developing a secure network architecture as a means to limit cyber threat actors' ability to exploit ICS, which is far easier when the systems are integrated and no zones or boundaries exist.[13] The Department of Homeland Security endorses developing a layered cyber defense consisting of five unique zones, as outlined in figure 14-1.[14]

12. Theodore Williams, "The Purdue Enterprise Reference Architecture," *IFAC Proceedings* 26, no. 2 (1993): 559–64, https://doi.org/10.1016/S1474-6670(17)48532-6.

13. Department of Homeland Security (DHS), *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies* (Washington, DC: DHS, 2016), 16–20, https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

14. DHS, *Recommended Practice*, 18.

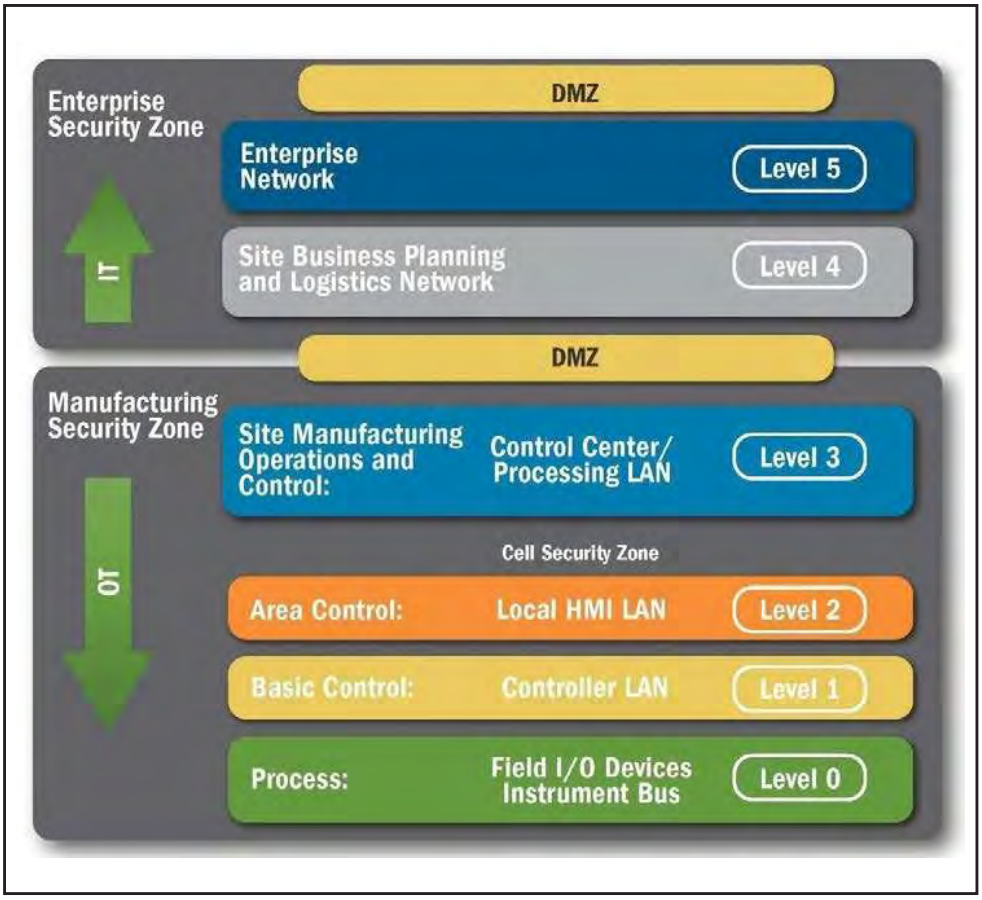

Figure 14-1. ICS reference model
(Diagram by US Department of Homeland Security)

The first section, the enterprise security zone, is not directly related to the ICS. This zone provides employees the connectivity to the Internet, remote sites, and business networks that comprise the intranet, e-mail servers, web servers, and other business systems. The enterprise security zone is also known as the informational technology (IT) system. See chapter 3 for its helpful explanation of operational and informational technology [OT and IT] systems. Next, the manufacturing security zone is where a vast majority of monitoring and control takes place. Depending on the size of the ICS, this zone may contain multiple cell zones. The third section, the cell zone, contains local human-machine interfaces (HMI), controllers, and field devices to be monitored and controlled. The HMI is a desktop computer with control software through which operating personnel manipulate the ICS. The cell zone also may include a safety instrumented system, which is a special controller designed to automatically take actions in the event

of dangerous conditions like excessive pressure or temperature. Fieldbus protocols with hard wiring are typically used between field devices and controllers, whereas Ethernet is common between controllers and HMIs. Finally, a demilitarized zone (DMZ) is a subnetwork that acts as an intermediary to protect the inside network. Within the ICS, the DMZ is where the data historian, antivirus or patch, and remote access gateway are located. A data historian is a time-series database to capture all production and process data for monitoring and analysis troubleshooting.

Security Concerns in ICS

In the past, critical infrastructure facilities operated ICS strictly in a closed network environment. To ensure real-time monitoring and efficient and effective resource planning at the enterprise level, however, the prevalent practice in modern critical infrastructure is to operate ICS in a more open, interconnected network with business networks. Examples of business applications that may connect to ICS include production planning and scheduling applications, manufacturing execution systems, inventory management systems, and maintenance management systems.[15] Furthermore, the Ethernet and other open standard technologies are also becoming more prevalent in ICS. As a result, attackers can understand and exploit system components more easily than they could in the past. These realities raise security concerns because ICS are more vulnerable to cyberattacks than ever before. When compared to IT systems, the following system characteristics make it more challenging to secure ICS in the face of the numerous vulnerabilities, risks, and threats in the cyber domain.[16]

- Timeliness and performance requirements. As ICS are usually time-critical, security measures causing an unacceptable delay and/or threatening the functionality of the system cannot be deployed.
- Availability requirements. Patches cannot be applied on time as they have to be tested thoroughly for stability and reliability. Outages of systems to install patches typically must be scheduled weeks in advance.
- Risk management requirements. Security measures that impair safety are unacceptable.

15. Eric D. Knapp and Joel T. Langill, *Industrial Network Security* (Waltham, MA: Syngress, 2014), 20.
16. NIST, *Guide to Industrial Control Systems*, 2-14–2-17.

- Physical effects. As ICS have complicated physical processes, good communications between experts in the control system and the physical domain are necessary.
- System operation. Since ICS operating systems and networks are often quite different from IT counterparts, they require different skill sets, experience, and levels of expertise.
- Resource constraints. Many components are resource-constrained in memory and processing power. As a result, typical contemporary security capabilities may not apply.
- Communications. Communication protocols and media for field devices (sensors and actuators) are different from those used in IT environments and thus require other specialties.
- Managed support. Given the fact that maintenance is often performed by a single vendor, the use of third-party solutions requires the vendor's approval or the ICS will no longer be under warranty.
- Component lifetime. The lifetime of the ICS components is often over 15 years, while IT components require upgrades and patches much more frequently.
- Component location. In some cases, ICS components may be located at remote sites that require extensive transportation effort to reach. Each site needs to be appropriately protected.

Beyond the limitations and restrictions in applying sufficient security measures due to the inherent nature of ICS, there are also several security concerns and problems commonly found in most ICS.

Vulnerabilities in ICS Components

According to a recent cybersecurity survey, organizations disclosed 893 vulnerabilities specific to their ICS in 2020—a steady increase from the 672 reported in 2018 and the 716 in 2019.[17] Surprisingly, in 76 percent of these disclosed vulnerabilities, threat actors were able to launch attacks without needing to be authenticated. These figures, however, do not include vulnerabilities found in common IT components, such as employees' personal desktops, servers, databases, and network switches.

17. Claroty Research Team, *Claroty Biannual ICS Risk & Vulnerability Report: 2H 2020* (New York: Claroty, 2020), 4–11, https://security.claroty.com/biannual-ics-risk-vulnerability-report-2H-2020.

These components are predominantly commercial-off-the-shelf products or custom-made models based on these products. Traditionally, vendors have not considered security an integral part of a product development process, but this dynamic is changing. Despite the recent rise in concern regarding security of control system components during product development, the level of security in ICS lags behind and is not as comprehensive when compared to the security of IT products.[18] Therefore, there are many weaknesses in ICS components, including susceptibility to denial-of-service attacks and lack of security checks for firmware updates. Even IT components used in control systems are often configured to enable insecure services, such as Telnet, by default.[19]

ICS Components Exposed to the Internet

Many ICS components are connected to the Internet without proper security measures like firewalls or remote access gateways. In 2019, a search on Shodan—a special search engine often used to find devices connected to the Internet—revealed more than 2.6 million ICS components around the globe were connected to the Internet.[20] Most of these devices were likely used in schools for research or by small private companies. Poor security practices or breaches in security protocols (such as opening a firewall port for remote access and then forgetting to close it or connecting to the Internet intentionally to reduce work burdens) may occur even in national critical infrastructure, making these facilities and organizations equally vulnerable.

Connection with Business Systems

According to the SANS Institute's 2019 survey of 338 organizations, 57 percent connected their ICS to business systems while 35 percent connected their ICS to the Internet either through the DMZ or directly.[21] When such a connection is inevitable, it must be secured to prevent malicious traffic from entering the ICS network. A firewall can be used for this purpose, but a unidirectional network device—a special security gateway that is also

18. DHS, *Recommended Practice*, 4.

19. Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats* (New York: Momentum Press, 2010), 29.

20. David Hasselquist, Abhimanyu Rawat, and Andrei Gurtov, "Trends and Detection Avoidance of Internet-Connected Industrial Control Systems," *IEEE Access* 7 (2019): 155504–12, https://doi.org/10.1109/ACCESS.2019.2948793.

21. Barbara Filkins, *SANS 2019 State of OT/ICS Cybersecurity Survey* (Rockville, MD: SANS Institute, 2019), 12.

known as a data diode—is the optimal solution because it is allows data to travel in only one direction.[22] Organizations may also consider using an intrusion detection system (IDS). Even if such security devices are in place, however, there is still a risk of allowing malicious traffic due to misconfiguration. Moreover, an IDS cannot be used if the control system vendor does not approve because of potential degradation in network performance. An IDS is more commonly found in IT networks than in ICS networks and, even when installed, it may not be able to fully understand ICS protocols.[23]

Outdated Components

As an ICS typically has a very long lifespan, it is common to find ICS components already past end of life, such as when HMIs run on outdated programs like Windows XP or 7. Even if organizations want to upgrade old components, they cannot be upgraded if application software does not support the latest operating system or the vendor does not guarantee reliability after an upgrade. Installing antivirus programs on old desktops may not be feasible because of performance and stability issues. Moreover, when old hardware is damaged, it may not be easy to find replacement options that meet the same specifications.

Remote Access to Control Networks

With the recent development of cloud technology, cloud-based management services for IT systems have emerged, and similar movements are also emerging for ICS. According to the 2019 SANS survey previously cited, more than 40 percent of respondents used cloud-based services for their ICS. Respondents gave three main reasons for why they used these services: (1) remote monitoring, (2) configuration, and (3) analysis, which accounted for 44 percent of the reported uses.[24] Regardless of the types of outsourced services, all remote accesses must be controlled in a highly secure manner.

Insecure Nature of ICS Protocols

All major fieldbus protocols—such as Modbus, DNP3, Profinet, and EtherCAT—are susceptible to man-in-the-middle attacks because they generally lack sufficient authentication or encryption.[25] Such attacks can disrupt network operations or manipulate input-output messages

22. NIST, *Industrial Control Systems*, 5–21.

23. European Union Agency for Cybersecurity (ENISA), *Communication Network Dependencies for ICS/SCADA Systems* (Athens: ENISA, 2016), 30, https://www.enisa.europa.eu/publications/ics-scada-dependencies/.

24. Filkins, *OT/ICS Cybersecurity Survey*, 13–14.

25. Knapp and Langill, *Industrial Network Security*, 166.

to cause failure. Protocol gateways, including serial-to-Ethernet converters, that translate one ICS protocol to another could provide an additional attack vector as they may contain security flaws and vulnerabilities.[26]

Major Cyber Incidents

Due to insecure configuration and management, cyber incidents in ICS have unfortunately become a common occurrence. This section will now examine some of the significant cyberattacks that targeted ICS.

Stuxnet (2010)

The most historic cyber incident associated with ICS was the infection of Iran's nuclear program with Stuxnet, a worm designed to penetrate air-gapped control networks via USB flash drives and then propagate through self-replication. The Stuxnet worm, which was discovered in 2010, precisely targeted the centrifuges used in Iran's uranium enrichment process to change the frequencies of the frequency converters covertly that adjust motor speed. It is activated only when the same software—namely, Siemens WinCC and Step7—and frequency range as the Iranian facility are found.[27] While the physical consequences of Stuxnet were limited in that Iran took just one year to recover fully from the effects of the attack, this incident demonstrated that separating the ICS network from the Internet can no longer be considered a sufficient security measure.[28]

BlackEnergy (2011)

In 2014, the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) alerted that BlackEnergy malware had been targeting users of HMI products, such as GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC, since 2011.[29] Attackers targeted the Internet-connected HMIs and then exploited a vulnerability of the software to install BlackEnergy

26. Marco Balduzzi et al., *Lost in Translation: When Industrial Protocol Translation Goes Wrong* (Irving, TX: Trend Micro, 2020), 48–49, https://i.blackhat.com/USA-20/Wednesday/us-20-Balduzzi-Industrial-Protocol-Gateways-Under-Analysis-wp.pdf.

27. William Maclean, "Stuxnet Study Suggests Iran Enrichment Aim: Experts," Reuters (website), November, 16, 2010, https://www.reuters.com/article/us-security-cyber-stuxnet-idUSTRE6AF2F320101116.

28. Marie Baezner and Patrice Robin, "CSS Cyber Defense Hotspot Analysis Issue 4: Hotspot Analysis: Stuxnet," Center for Security Studies at ETH Zurich (website), October 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf.

29. "ICS Alert: Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)," Cybersecurity and Infrastructure Security Agency (CISA) (website), July 22, 2021, https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-14-281-01B.

malware. Although no malicious activity was identified, the malware could have damaged, modified, or disrupted the targeted systems. A security company found that some of the command and control (C2) servers used in this attack were the same as those used by the Russian Advanced Persistent Threat (APT) group known as Sandworm.[30] In July 2021, the US government officially attributed the BlackEnergy attack to Russian nation-state cyber actors.[31]

Havex (2013)

The Russian APT group known as Dragonfly used Havex in a cyber espionage campaign targeting ICS in a variety of countries, including several NATO member states.[32] Havex is a remote access Trojan that leveraged the Open Platform Communications—the data exchange protocol between Windows systems and controllers—to collect information on the targeted devices. The attackers Trojanized software available for download from three ICS manufacturer websites and gained access to the networks of systems that had installed the software.[33] A security company later found 88 variants were communicating with 146 C2 servers, which made connections with 1,500 different Internet Protocol addresses, each of which represents a possible victim of the attack.[34] Although the primary usage of Havex was espionage, its C2 server could have also been used in other attacks.[35] In 2021, the US government attributed the Havex attacks to Russia.[36]

German Steel Mill (2014)

According to the annual report issued in 2014 by Germany's Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, or BSI), unspecified threat actors attacked a German steel mill, compromising individual ICS components and causing a furnace to shut down

30. Kyle Wilhoit and Jim Gogolinski, "Sandworm to Blacken: The SCADA Connection," *Trend Micro* (blog), October 16, 2014, https://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/.

31. "Ongoing Sophisticated Malware Campaign."

32. Symantec, *Dragonfly: Cyberespionage Attacks against Energy Suppliers* (Mountain View, CA: Symantec, 2014), 5, https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers.

33. "ICS Advisory (ICSA-14-178-01): ICS Focused Malware," CISA (website), updated on July 20, 2021, https://us-cert.cisa.gov/ics/advisories/ICSA-14-178-01.

34. Daavid Hentunen and Antti Tikkanen, "Havex Hunts for ICS/SCADA Systems," F-Secure Labs (website), June 23, 2014, https://archive.f-secure.com/weblog/archives/00002718.html.

35. "ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack against Ukrainian Critical Infrastructure," CISA (website), updated July 20, 2021, https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01.

36. "ICS Focused Malware."

in an abnormal manner.[37] The attackers used spear-phishing e-mails to steal login credentials and then used them to gain access to the mill's control system.

Ukraine Blackout (2015)

The Ukraine blackout in December 2015, which caused electricity disruption to 225,000 people in western Ukraine for up to six hours, was the first known successful cyber intrusion to take a power grid offline and one of the most severe incidents in cybersecurity history. The attackers, part of the Sandworm group, conducted a remote intrusion into three power distribution companies.[38] The attackers reportedly used spear phishing to obtain credentials in advance, which enabled the intrusion into the companies and then to the various substations.[39] Moreover, they infected Windows systems with KillDisk malware to erase files and the master boot record and corrupted the firmware of serial-to-Ethernet converters at substations to make them inoperable. As with the BlackEnergy and Havex attacks, the US government also attributed the 2015 blackout to Russia.[40]

RWE's Nuclear Power Plant, Germany (2016)

Computer viruses Conficker and W32.Ramnit were discovered in German utility company RWE's nuclear power plant near Munich in April 2016. The infected system was a computer used to view the movement of nuclear fuel rods, but the infection did not cause any harm as the plant was disconnected from the Internet.[41] The same malware was found on 18 removable drives used for office computers, implying that at least one of the office drives was inserted into the infected system. The official investigation also concluded the malware probably came from a USB drive.[42]

37. *Bundesamt für Sicherheit in der Informationstechnik* (BSI), *Millionenfacher Identitätsdiebstahl in Deutschland* (Bonn: BSI, 2014), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf.

38. Michael Assante, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," SANS Institute (website), January 6, 2016, https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/.

39. "Cyber-Attack against Ukrainian Critical Infrastructure."

40. "Cyber-Attack against Ukrainian Critical Infrastructure."

41. Christoph Steitz and Eric Auchard, "German Nuclear Plant Infected with Computer Viruses, Operator Says," Reuters (website), April 26, 2016, https://www.reuters.com/article/us-nuclearpower-cyber-germany/german-nuclear-plant-infected-with-computer-viruses-operator-says-idUSKCN0XN2OS.

42. "Virus in the Gundremmingen Nuclear Power Plant Came from a USB Stick," CIO (website), June 3, 2016, https://www.cio.de/a/amp/virus-im-akw-gundremmingen-kam-ueber-usb-stick,3229370.

CrashOverride (2016)

During its cyberattack against a Ukrainian substation in December 2016 that caused a small-scale power outage, the Sandworm group used CrashOverride malware (also known as Industroyer).[43] This attack, like the several of the previous examples, was later attributed to Russian nation-state cyber actors.[44] Although this cyberattack was smaller in scale and duration than the one that caused the Ukraine blackout, CrashOverride was developed to create a far more widespread outage than the one that occurred in 2015. The CrashOverride malware has capabilities to issue malicious commands directly to remote terminal units—the controllers used for SCADA systems (such as power grids)—by exploiting the lack of authentication and authorization in the ICS protocol. The malware can also prevent legitimate communications with field devices, cause the shutdown of a relay, and employ its wiper module to render windows system inert and thus require a rebuild or backup restoration.[45] After the Stuxnet attack, the use of CrashOverride malware in 2016 is only the second known case of malicious codes intentionally built to disrupt physical systems. For a more detailed explanation and assessment of cyberattacks on Ukraine's power grid, see the overview provided in chapter 5.

TRITON (2017)

Following the mysterious shutdown of an entire petrochemical plant in Saudi Arabia in 2017, the subsequent investigation found the attackers gained remote access to an engineering workstation—a computer used for configuring a safety instrumented system (SIS)—using TRITON malware. TRITON, also known as TRISIS, is a malware that attacks the Triconex SIS fabricated by the company Schneider Electric. The TRITON malware allowed the attackers to reprogram the SIS, causing the controllers to shut down automatically.[46] Although it is not certain who is responsible for the cyberattack, evidence suggests Russia's Central Scientific Research Institute of Chemistry and Mechanics supported the development of TRITON.[47] In October 2020,

43. Assante, "Confirmation of a Coordinated Attack."

44. "Alert (TA17-163A): CrashOverride Malware," CISA (website), updated on July 20, 2021, https://us-cert.cisa.gov/ncas/alerts/TA17-163A.

45. "Alert: CrashOverride Malware."

46. Blake Johnson et al., "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure," *FireEye* (blog), December 14, 2017, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

47. FireEye Intelligence, "TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers," Mandiant (website), October 23, 2018, https://www.mandiant.com/resources/triton-attribution-russian-government-owned-lab-most-likely-built-tools.

the US Department of the Treasury imposed sanctions on this Russian research institution for its involvement with TRITON.[48]

Water Treatment Plant, United States (2021)

In February 2021, an unidentified attacker hacked the water treatment plant in Oldsmar, Florida. After accessing the plant remotely, the attacker tried to increase the level of sodium hydroxide in the water supply to 100 times greater than normal. Fortunately, operating personnel quickly spotted this abnormality and returned the sodium hydroxide to the normal level. The investigation later found the attacker accessed the system via remote access software called TeamViewer, which plant employees had installed and used to check system status and respond to alarms.[49] City officials noted that automated safeguards, such as pH testing, would have triggered an alarm before anyone was harmed, even if the employee had not noticed and stopped the attack.[50] The incident clearly showed, however, that sabotage attacks targeting national critical infrastructure could occur at any moment. For more information on the Oldsmar cyberattack, see chapter 8.

Colonial Pipeline (2021)

Colonial Pipeline, the largest pipeline company in the United States, had to shut down its 5,500-mile pipeline on the east coast for six days due to the ransomware attack by the Russian criminal group called DarkSide.[51] Since the pipeline typically transported more than 110 million gallons of fuel per day, the attack had devastating results: 88 percent of gas stations in Washington, DC, ran out of fuel as did more than 50 percent of gas stations in South Carolina, North Carolina, and Virginia.[52] Although the attack was targeted at IT systems only, the company had to halt its pipeline operation because it could not bill its customers. The fundamental issue

48. "Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware," US Department of Treasury, October 23, 2020, https://home.treasury.gov/news/press-releases/sm1162.

49. CISA, "Alert (AA21-042A): Compromise of U.S. Water Treatment Facility," February 12, 2021, https://us-cert.cisa.gov/ncas/alerts/aa21-042a.

50. Andy Greenberg, "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say," Wired (website), February 8, 2021, https://www.wired.com/story/oldsmar-florida-water-utility-hack.

51. "FBI Statement on Compromise of Colonial Pipeline Networks," Federal Bureau of Investigation (website), May 10, 2021, https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks.

52. Jonathan Garber, "Colonial Pipeline Fiasco Foreshadows Impact of Biden Energy Policy," Fox Business (website), May 15, 2021, https://www.foxbusiness.com/markets/colonial-pipeline-fiasco-foreshadows-impact-of-biden-energy-policy.

with this incident is that the data necessary for pipeline operations should not be resident on the IT network.[53]

Security Recommendations for ICS

To defend against cyberattacks targeting a critical infrastructure's ICS, organizations need to have good cyber hygiene practices and properly implemented defensive techniques.[54] This section provides an overview of basic cyber hygiene practices and recommended ICS security measures.

Basic Cyber Hygiene Practices

As a fundamental principle of cybersecurity, proper cyber hygiene establishes simple and routine measures to reduce risks from cyber threat actors.[55] In the United Kingdom, a government report in 2015 indicated that 80 percent of cyberattacks could have been prevented if organizations had implemented simple security controls.[56] Although this percentage is not specific to attacks against an organization's ICS, a similar 80-20 rule can be equally applied. Most of the incidents mentioned above were due to inadequate security practices, such as connecting an ICS to the Internet or business network without proper security measures, leaving remote access points open without monitoring, and lack of security controls over removable drives.

There is no clear scope for cyber hygiene. According to a survey on cyber hygiene practices conducted by the European Union Agency for Cybersecurity (ENISA), cyber hygiene generally includes these common practices.[57]

- Identification of hardware and software to determine what to manage.
- Application of secure configuration and hardening for all devices.

53. Joe Weiss, "The Colonial Pipeline Cyberattack—Did IT/OT Convergence Contribute to the Attack," *Control Global* (blog), May 11, 2021, https://www.controlglobal.com/blogs/unfettered/the-colonial-pipeline-cyberattack-did-itot-convergence-contribute-to-the-attack/.

54. "Alert: CrashOverride Malware."

55. ENISA, *Review of Cyber Hygiene Practices* (Athens: ENISA, 2016), 5, https://www.enisa.europa.eu/publications/cyber-hygiene/.

56. Department for Business, Innovation and Skills, "Cyber Security Boost for UK Firms," GOV.UK (website), January 16, 2015, https://www.gov.uk/government/news/cyber-security-boost-for-uk-firms.

57. ENISA, *Review of Cyber Hygiene Practices*, 15.

- Patching systems to keep them current.
- Management of inbound and outbound data.
- Scanning of all incoming e-mails.
- Minimization of the number of administrative accounts.
- Conduct of regular data backup.
- Establishment of an incident response plan.
- Enforcement of security across the supply chain.
- Placement of appropriate security controls in any service agreements.

Similar to these recommended measures in the EU, the US Cybersecurity and Infrastructure Security Agency (CISA) published its Cyber Essential Starter Kit in 2021 to promote basic cyber hygiene practices and a strong culture of cyber readiness. The CISA guide highlights essential steps for an organization to establish cyber readiness in six key areas: management, employees, critical systems, surroundings, data, and an incident response plan.[58]

Essential Cybersecurity Measures Specific to ICS

As Allies and partners consider how to enhance their cybersecurity posture, there are many guidelines, references, and standards that ICS operators and system integrators can refer to for ICS cybersecurity next steps and recommendations. Representing a spectrum of perspectives and best practices employed in various NATO member states, such documents include:

- Canada and the United States: North American Electric Reliability Corporation's Critical Infrastructure Protection Standards[59]
- EU: ENISA's Protecting Industrial Control Systems[60]

58. CISA, *Cyber Essential Starter Kit* (Washington, DC: CISA, 2021), 2, https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf.

59. "CIP Standards," North American Electric Reliability Corporation (website), n.d., accessed on November 5, 2021, https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

60. ENISA, *Protecting Industrial Control Systems* (Athens: ENISA, 2011), https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states/.

- France: The National Cybersecurity Agency's (ANSSI) Detailed Measures: Cybersecurity for Industrial Control Systems[61]
- Germany: Federal Office for Information Security's (BSI) ICS Security Compendium[62]
- International: International Electrotechnical Commission 62443 standard series, which currently includes nine standards, technical reports, and technical specifications to secure industrial automation and control systems[63]
- United States:
  - DHS's Catalog of Control Systems Security: Recommendations for Standards Developers[64]
  - DHS's Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies[65]
  - National Institute of Standards and Technology's Guide to Industrial Control Systems Security[66]

As these documents contain vast amounts of information, it is not feasible to examine them more thoroughly in this chapter. Instead, a more helpful framework for Allies and partners seeking to strengthen the security and resilience of ICSs in their critical infrastructure is the *Seven Steps to Effectively Defend ICSs*. After assessing the nearly 300 reported cyber intrusions in 2015, this DHS report identifies seven essential security principles that could have

61. *Agence nationale de la sécurité des systèmes d'information* (ANSSI), *Detailed Measures: Cybersecurity for Industrial Control Systems* (Paris: ANSSI, 2014), https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_detailed_measures.pdf.

62. BSI, *ICS Security Compendium* (Bonn: BSI, 2013), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.html.

63. "Understanding IEC 62443," International Electrotechnical Commission (website), February 26, 2021, https://www.iec.ch/blog/understanding-iec-62443.

64. DHS, *Catalog of Control Systems Security: Recommendations for Standards Developers* (Washington, DC: DHS, 2011), https://us-cert.cisa.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf.

65. DHS, *Recommended Practice.*

66. NIST, *Guide to Industrial Control Systems.*

prevented 98 percent of these incidents.[67] The principles and corresponding security measures outlined in the DHS report are listed below.[68]

- Implement application whitelisting. This step allows only applications and programs predesignated by an administrator to execute, effectively preventing the execution of malware.
- Ensure proper configuration and patch management. Since unpatched systems are more vulnerable to adversaries, this step emphasizes the import and implementation of trusted patches. It includes tracking required patches for each IT asset, obtaining updates from verified sources, validating their authenticity against digital signatures and hash values, testing them on a system equipped with malware detection features, and limiting the connection of external laptops to ICS.
- Reduce attack surface areas. To minimize vulnerabilities, this step seeks to isolate the ICS network from any untrusted networks, lock down all unused ports, disable all unused services, limit external connectivity, use one-way communications for external connectivity if applicable, and employ measures such as restricting a network port or path when bidirectional communications are necessary.
- Build a defendable environment. To limit damages due to breaches of the network, this step calls for segmenting networks into smaller logical enclaves (virtual LANs), restricting host-to-host communications paths, and using a secure means for data transfer from control networks to business networks.
- Manage authentications. Since adversaries seek to gain control of legitimate credentials, this step aims to limit this illegitimate access. Key steps include implementing multifactor authentications when possible, granting users the fewest privileges required to complete duties, enforcing strong password management policies, and not sharing authentication servers between ICS and business networks when centralized authentication is used.

67. DHS, *Seven Steps to Effectively Defend ICSs* (Washington, DC: DHS, 2015), 1–2, https://us-cert.cisa.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf.

68. DHS, *Seven Steps to Defend ICSs*, 2–5.

- Implement secure remote access. To counter adversarial attempts to gain unauthorized access to ICSs, this step aims to remove remote access wherever possible. Important actions include limiting any access that remains continuously, implementing read-only access using hardware-type unidirectional network devices, requiring remote access to be time limited and controlled by operating personnel, applying the same remote access paths for vendors and employees, and using two-factor authentication with different types of tokens.
- Monitor and respond. In the modern cyber operating environment, active monitoring is essential. This step recommends monitoring Internet Protocol traffic on ICS boundaries and within the ICS networks, using host-based security solutions to detect malicious software, reviewing login activities to detect stolen credential usage, monitoring changes in access controls, and establishing a sound response plan.

Regarding current threats and vulnerabilities, and the corresponding security measures to mitigate them, various organizations worldwide—including cybersecurity authorities, computer emergency response teams, computer security incident response teams, ICS vendors, and security companies—are continuously issuing advisories, warnings, alerts, and reports. ICS operators and system integrators can stay up to date on evolving cyber threats and appropriate security measures by referencing these documents.

Risk Management for ICS Cybersecurity

The process of risk management is a fundamental task to achieve cybersecurity because it can identify assets that are exposed to risks, assess the level of these risks, implement appropriate measures commensurate with the levels of risks, and continuously monitor and manage the effectiveness of these mitigation steps. When considering risk management practices for IT systems in general—not ICSs in particular—perhaps the most authoritative standard document is *Information Security Risk Management* (ISO/IEC 27005).[69] This document supplements *Information Security Management Systems—Requirements,* the international standard for establishing,

69. *Information Security Risk Management,* ISO/IEC 27005 (Geneva: International Organization for Standardization, 2018), https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en.

implementing, operating, monitoring, and maintaining IT security.[70] As depicted in *Information Security Risk Management*, the general risk management process consists of five essential steps, which are outlined below.

- Context establishment. This steps involves preparation activities, such as setting basic criteria, defining the scope, and establishing a risk management team. The basic criteria include risk evaluation criteria (how to evaluate risks), impact criteria (how to measure impacts), and risk acceptance criteria (thresholds for a desired target level of risk).
- Risk identification. This stage begins with the identification of assets, to include hardware, software, data, information, systems, and process. Then it proceeds with identifying the following information: threats to these assets, existing countermeasures, vulnerabilities that threats can exploit, and potential consequences or damage that could result.
- Risk analysis. This step can be performed in varying degrees of detail. Its methodology can be qualitative—the magnitude and likelihood of an incident are described as low, medium, or high—or quantitative, which uses numerical values rather than descriptions. A combination of likelihood and consequence determines the level of risk for each incident.
- Risk evaluation. This stage helps determine whether risk treatment activities should be carried out for each risk and prioritizes the activities in order of risk level.
- Risk treatment. There are four options available for risk treatment. First, risk modification looks to implement security measures to mitigate risks to an acceptable level by referencing a set of standards and best practices. Next, risk retention accepts risks only when the consequences are negligible or within a range of tolerated outcomes. Third, risk avoidance leads stakeholders to change conditions or cease activities that encounter risks. Finally, risk sharing employs methods like insurance to prepare for residual risks that remain.

Information Security Risk Management recommends organizations perform the risk management process iteratively, starting from an initial high-level assessment to succinctly identify the most critical risks with a broader view.

70. *Information Security Management Systems—Requirements*, ISO/IEC 27001 (Geneva: International Organization for Standardization, 2013), https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

Organizations should then perform a detailed assessment that comprehensively analyzes assets, vulnerabilities, threats, and consequences in the second iteration and beyond. Furthermore, organizations should perform risk management regularly, given the evolving nature of the modern security environment. See the thorough explanation of the risk assessment and management process outlined in chapter 13.

Risk Assessment Methodology for ICS

In 2020, the International Electrotechnical Commission published the international standard for ICS risk assessment—*Security Risk Assessment for System Design* (IEC 62443-3-2)—and adopted it as part of the broader *Security for Industrial Automation and Control Systems series.*[71] A key concept in *Security Risk Assessment for System Design* is the consideration of ICS zones and conduits. A zone is a collection of logical and physical assets posing the same characteristics from the perspective of security requirements, criticality, and logical and physical relationships. A conduit is a logical grouping of communications channels that have the same security requirements, and each conduit represents the connection between two or more zones.

Another distinguishing aspect of IEC 62443-3-2 is that it utilizes the concept of security level (SL)—a measure of confidence that the ICS is free from vulnerabilities and is functioning as intended—to assist organizations in identifying required security measures. Derived from the international standard *System Security Requirements and Security Levels* (IEC 62443-3-3), a standard practice is to assign a label to each security measure ranging from SL1 (basic security) to SL4 (most sophisticated security).[72] After assigning these labels, organizations then use them to identify recommended security measures commensurate with their target level of protection. For example, as for the security requirements related to "system log storage capacity," IEC 62443-3-3 suggests that using a storage with sufficient capacity would be just sufficient for SL1 and that a warning function against low disk space should be added to achieve SL2 or above.

Similar to the iterative approach used in *Information Security Risk Management,* the ICS risk assessment process outlined in IEC 62443-3-2 is also divided into two levels, namely, initial risk assessment and detailed

71. *Security for Industrial Automation and Control Systems—Part 3-2: Security Risk Assessment for System Design*, IEC 62443-3-2 (Geneva: International Electrotechnical Commission, 2020), https://webstore.iec.ch/publication/30727.

72. *Industrial Communication Networks—Network and System Security—Part 3-3: System Security Requirements and Security Levels*, IEC 62443-3-3 (Geneva: International Electrotechnical Commission, 2013), https://webstore.iec.ch/publication/7033.

risk assessment. The process for ICS risk assessment consists of seven steps, which are described below and illustrated in figure 14-2.

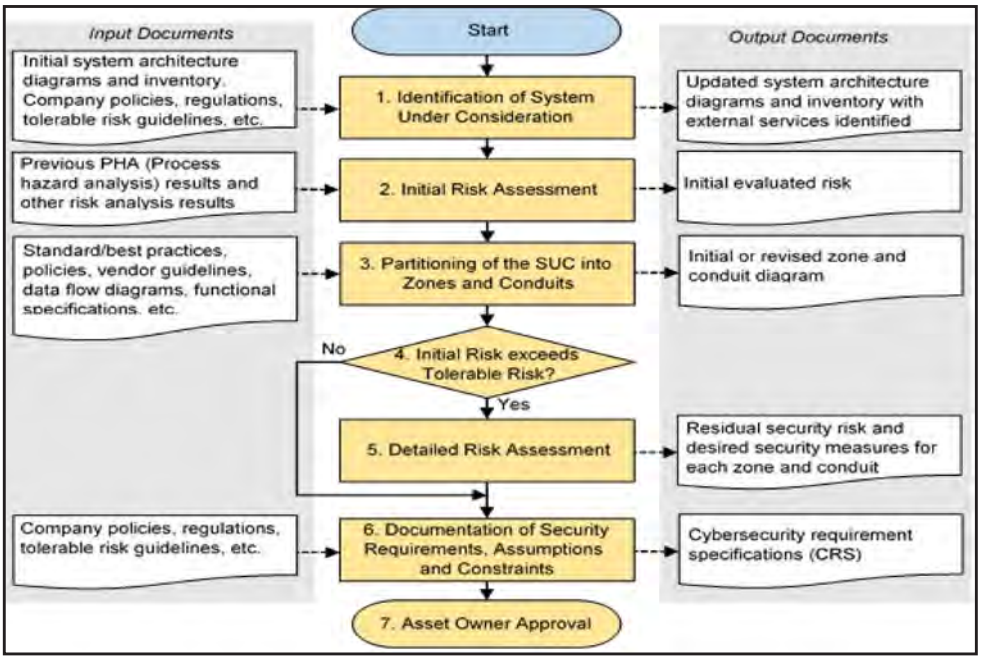

Figure 14-2. Workflow diagram for ICS risk management
(Diagram by the International Electrotechnical Commission)

- Identification of system under consideration (SUC). Step 1 identifies the SUC, including identification of the ICS boundary, access points, and all ICS assets.
- Initial risk assessment. Step 2 identifies the worst-case scenarios by assuming the likelihood of occurrence to be 100 percent certain. The purpose of the initial assessment is to identify and prioritize the areas for detailed assessments.
- Partitioning of the SUC into zones and conduits. Step 3 includes a grouping of ICS assets based on the initial assessment results so that assets with the same characteristics are grouped into the same zones. Organizations are recommended to group unordinary devices (such as wireless devices and devices connected to external networks) into separate zones because they require special care.

- Risk comparison. In Step 4, organizations determine if an additional detailed risk assessment is required for the SUC (or part of it) by comparing the initial assessed risk to the level of risk the organization can tolerate. If the assessed risk exceeds the tolerable risk, then the organization should perform a detailed risk assessment.
- Detailed risk assessment. Step 5 builds on the previous steps and goes into greater examination of the system, using a series of micro-steps. Here, organizations (1) identify all threats that could affect the assets within the zone or conduit, (2) identify areas in which assets are vulnerable to these threats, (3) develop a worst-case estimate of potential impacts, (4) estimate the likelihood of such incidents occurring, (5) assess the level of risk for each threat, (6) compare the assessed risk to the tolerable risk to determine whether to accept, transfer, or mitigate the risk, (7) assess residual risks that remain after applying mitigation measures, and (8) identify additional measures when the residual risks exceed the tolerable risks.
- Documentation of security requirements, assumptions, and constraints. Step 6 is about documenting all the findings from previous steps. The cybersecurity requirements specification contains the description of mandatory security measures as well as details of the SUC, zones and conduits, threat environments, organizational policies, and tolerable risks.
- Asset owner approval. At the final step of each iteration of risk assessment, asset owners in charge of the safety and reliability of control processes review and approve the result.

Detailed Risk Assessment Approach

Since it provides an in-depth understanding of the nature of risks, a detailed approach to risk assessment is at the heart of managing risks to ICS and securing them more effectively. The risk assessment process requires an organization to estimate the likelihood of a threat and impacts of potential incidents for every pair of assets and threats. This process can be tedious and consume time and resources because it requires tremendous effort to have meaningful and valid results.

Qualitative or descriptive measures such as *high*, *medium*, and *low* can be used in estimation; however, they still require a detailed guideline to reduce subjective and ambiguous judgments as much as possible. Moreover, the impact has multiple attributes, requiring in-depth review from various perspectives, such as an outage of service, loss of process accuracy, and the impacts on health, safety, and environment. Once the organization estimates the maximum potential magnitude of impact and its likelihood for every asset-threat pairing, the organization can then determine the level of risk.

Qualitative analysis, on the other hand, uses simple mapping logics to determine the risk level. For instance, the risk is high if the likelihood and impact are both assessed as high. These logics are generally expressed in a matrix, called the *risk matrix*, with rows representing qualitative values for likelihoods and columns representing qualitative values of impacts. Quantitative analysis uses numerical metrics (such as annual loss expectancy), which is the monetary loss amount multiplied by the probability of occurrence. The measurement and assessment of risks serve as a basis of deciding which risks to prioritize in order of importance.

Scenario-based Approach for Security Baseline

For organizations with no experience or expertise in detailed risk assessment, the scenario-based risk mitigation approach may be helpful as a starting point toward developing more robust and effective ICS cybersecurity. This approach considers past incident cases or potential scenarios to identify required security measures to prevent such incidents from occurring. It can also be used to assess the effectiveness of the current security posture with relatively less time and resources.

Under the scenario-based approach, an organization first needs to identify assets, zones, and conduits within the ICS, and then build a catalog of threat scenarios applicable to them. To build a quality catalog of threat categories, organizations can compile incident reports and security warnings or advisories from various sources. Then, the organization should identify required security measures by referencing best practices and standards or by brainstorming with relevant stakeholders and experts. The next step is to evaluate the feasibility of the identified security measures. When any specific security measure cannot be implemented due to budget or technical restrictions, the organization should seek alternative or compensating controls (such as adding manual control procedures or physical controls).

The key advantage of the scenario-based approach is that no additional analysis skills are required for risk mitigation, so organizations can complete this type of assessment more quickly than a detailed risk assessment. The main disadvantage, however, is that some important risks could be overlooked, especially those risk scenarios that have not occurred elsewhere and thus are not considered as being in the realm of possible.[73] Another disadvantage is that there is little justification for chosen security measures from the viewpoint of cost-effectiveness because this approach does not consider the impact and likelihood of incidents. A robust catalog of threat scenarios could reduce these shortcomings to some extent.

When building a catalog of threat scenarios, Allies and partners may find the MITRE Corporation's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) for Industrial Control System (ICS) quite helpful as a tool and guide.[74] MITRE started building the ATT&CK for IT systems in 2013 and it is now widely accepted as a framework for documenting and analyzing tactics and techniques used by cyberattackers. MITRE's ATT&CK for ICS, launched in 2020, contains details of 78 attack techniques that threat actors employed in the wild along with corresponding mitigation measures organizations can take to enhance their cybersecurity posture. Another valuable source of information is the Top 10 Threats and Countermeasures for ICS, which the German BSI began publishing in 2014 to highlight the most severe but common cyber threats and outline appropriate security measures for organizations to adopt.[75]

Defending against Cyberattacks: Looking to the Future

The steps critical infrastructure owners and operators take to manage security risks and threats in their respective operational environments are vital to achieving cybersecurity. Their governments should also play a proactive role to build resilience and prepare for potential cyberattacks at both the national and international levels. The following section discusses the important efforts governments should undertake.

73. *Industrial Communication Networks—Network and System Security—Part 2-1: Establishing an Industrial Automation and Control System Security*, IEC 62443-2-1 (Geneva: International Electrotechnical Commission, 2010), 48, https://webstore.iec.ch/publication/7030.

74. "Techniques," MITRE Corporation (website), January 2, 2020, https://collaborate.mitre.org/attackics/index.php/All_Techniques.

75. BSI, *Industrial Control System Security Top 10 Threats and Countermeasures* (Bonn: BSI, 2019), https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf.

National-level Efforts for CISR

To varying degrees, national governments conduct cybersecurity governance activities through central ministries or authorities and develop and update their respective cybersecurity strategies that stipulate necessary measures to protect critical national infrastructure. In 2016, ENISA published a list of good practices through a detailed analysis of various governance activities across 15 EU member states. Some of the key practices that the report recommends EU member states adopt are listed below.[76]

- Partnerships with private stakeholders. As private companies manage many critical infrastructure systems and assets, it is essential to have a strong partnership between the government and the private sector in an institutional form, such as a national critical infrastructure protection committee or advisory meeting. See chapter 11 for its recommendations for public-private partnerships.
- Information-sharing scheme. Cyber threat information should be disseminated to all relevant government agencies and private critical infrastructure operators through preestablished information-sharing schemes. These established procedures allow relevant stakeholders to obtain up-to-date information promptly and take appropriate security measures.
- Develop the community of computer security incident response teams. Establishing the institutional foundation for cooperation among public and private response teams can lead to mutual benefits, such as increased knowledge and more efficient allocation of resources.
- Risk assessment. The government should guide and support private operators to identify risks and implement security measures as requested.
- Cyber crisis management. Cyber crisis management should include the definition of roles and responsibilities, and decision-making procedures between relevant stakeholders.

76. ENISA, *Stocktaking, Analysis and Recommendations on the Protection of CIIs* (Athens: ENISA, 2016), 16–19, https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis/.

- Comprehensive legal framework. Countries should have laws and regulations pertaining to securing critical infrastructure that stipulate the mandatory requirements for implementing essential security measures and notification of cyber incidents.

All of the steps listed above are important, but the most vital practice is information sharing. Private operators generally do not want their incidents to be disclosed to the public, while national and military intelligence agencies typically are reluctant to share their confidential information with the private sector. To overcome this problem, it is necessary to build trust that the shared information will never be leaked to other parties. The government should establish a formal information-sharing policy, including a sanitization process to remove sensitive content when disseminating information from a specific operator to other operators. Additionally, signing a nondisclosure agreement between parties can also build trust. For an in-depth discussion on helpful information- and intelligence-sharing practices, see chapter 11.

For effective and efficient dissemination of information, the government should use IT-based communications means. Depending on the size of the country, there may be thousands of critical infrastructure facilities, making the timely dissemination of threat information to all owners and operators almost impossible with manual handling procedures. In most situations, information technologies provide a more efficient and timely venue for multidirectional information sharing between the government and all relevant stakeholders. There are two examples of such programs used in the United States: the Homeland Security Information Network (HSIN) and the Automated Indicator Sharing (AIS), operated by the DHS and the CISA, respectively. The HSIN is an information portal for trusted information sharing between federal, state, local, international, and private-sector partners.[77] In contrast to the HSIN, the AIS is a real-time automated dissemination mechanism that sends machine-readable cyber threat indicators of compromise—artifacts observed on a network or operating system that indicate a cyber intrusion—to the participants of the AIS community.[78] Examples of these indicators include Internet Protocol addresses, domain names of C2 servers, and hash values of malware.

Beyond the recommendations in the ENISA report, two additional best practices are the use of cyber exercises and supply-chain security.

77. "Homeland Security Information Network (HSIN)," DHS (website), December 3, 2021, https://www.dhs.gov/homeland-security-information-network-hsin.

78. "Automated Indicator Sharing," CISA (website), n.d., accessed on October 23, 2021, https://www.cisa.gov/ais.

Since critical infrastructure systems and sectors are highly interrelated, an attack on a particular facility can affect other infrastructures rather than simply being confined to the initial target of the attack. In particular, attacks against the lifeline sectors (such as electricity and telecommunications) may affect all other sectors. To prepare for national-level cyber crises, the government should host exercises regularly with all relevant stakeholders. These exercises should include the procedures of decision making and communications across all government areas as well as the procedures for individual operators to respond to cyberattacks and report them to the government. *Cyber Storm*, which focuses on cyberattack crisis management, is the largest cyber exercise in the United States.[79] Similarly, *Cyber Europe i*s a large-scale cyber exercise that tests procedures, communications, and decision making at the EU level.[80]

Supply-chain security is a relatively new area of concern. The supply chain of hardware and software used for critical infrastructure should be protected against intentional and accidental modification that could be incurred during entire life cycles of products, including development, delivery, and maintenance. Malicious interference by a nation-state in cooperation with manufacturers located in its territory—by implanting a backdoor within IT/OT components, for example—is incredibly difficult to discover. Moreover, criminal or terrorist groups can also cause harm to IT/OT components by infiltrating manufacturers' development environments to modify source codes. Therefore, the government should establish a framework to screen the trustworthiness of manufacturers and ensure the security of products for their entire life cycles.

International-level Efforts for CISR

International cooperation is also essential to protect critical infrastructure because of the borderless nature of cyberspace. It is almost impossible for a single country to thoroughly analyze cross-border attacks and block further ones because attacks generally take place over multiple stages across several countries. Moreover, one country may possess intelligence that another country does not have. A complete analysis, investigation, and attribution of an attack thus require close international cooperation. Ideally, all government agencies involved in securing critical infrastructure (such as the national cybersecurity authority, national and military intelligence

79. "Cyber Storm: Securing Cyber Space," CISA (website), n.d., accessed November 3, 2021, https://www.cisa.gov/cyber-storm-securing-cyber-space.

80. "Cyber Europe," ENISA (website), n.d., accessed on November 3, 2021, https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

agencies, cyber commands, law enforcement agencies, and computer security incident response teams) should have close international cooperation channels with relevant counterparts in foreign countries. Multilateral treaties or agreements—like the Convention on Cybercrime of the Council of Europe, also known as the Budapest Convention—can play a crucial role since all members would be obliged to cooperate without having to make separate bilateral agreements with each other.[81] The Budapest Convention, currently signed by 66 countries, is the international treaty on cybercrimes to obtain a series of powers and procedures required for law enforcement. Article 23 of the convention stipulates that international cooperation is to be provided among participants to the widest extent possible.

Likewise, participating in international malware information-sharing platforms (MISP), such as the MISP sponsored by NATO and the EU, will provide the participating countries with up-to-date global threat information and relevant indicators of compromise on a real-time basis.[82] MISP is an open-source information-sharing platform developed by a team of cybersecurity experts from the Computer Incident Response Center in Luxembourg, the Belgian Ministry of Defense, and NATO. MISP can share, store, and correlate indicators of compromise, threat intelligence, vulnerability information, and even counterterrorism information.[83] Allies and partners may also consider participating in HSIN and AIS, as access can be granted to non-US entities under certain conditions.

Areas for international cooperation are not limited to exchanging threat information, sharing intelligence, and supporting investigations. Instead, it should include exchanges of various cybersecurity know-how and best practices, such as lessons learned from certain types of cyber incidents, detailed information on technical cybersecurity measures, policies for securing supply chains against cyber threats, and tools for assessing an organization's cybersecurity level. As countries exchange such information and provide technical support and consultation to one another, if requested, their cooperation will help build common capabilities to achieve cyber security, defense, and resilience at sufficient levels to secure critical national infrastructure. International cooperation is of paramount

81. "Details of Treaty No. 185," Council of Europe (website), n.d., accessed November 3, 2021, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

82. "Who Is behind the MISP Project?," MISP Threat Sharing (website), n.d., accessed on November 5, 2021, https://www.misp-project.org/who/.

83. "What Is Malware Information Sharing Platform (MISP)?," Cyware (website), September 17, 2020, https://cyware.com/educational-guides/cyber-threat-intelligence/what-is-malware-information-sharing-platform-misp-b28e.

importance in general, but especially for EU member states, because many European critical infrastructure sectors and systems are interconnected. The European power grid as well as oil and gas pipelines are two key examples of this connectivity.[84] An incident in one country may affect other countries, potentially leading to a cascade effect. See chapter 12 for more detail on the nature of dependencies and interdependencies among critical infrastructure sectors.[85]

Conclusion

This chapter provided a brief overview of the characteristics of ICSs, major cyber incidents against ICSs, essential cybersecurity measures, and risk management methodologies. Cyber incidents against critical infrastructure continue to occur due to inadequate security management practices, system misconfigurations, and human errors. Since critical infrastructure plays an important role in social well-being and national security, operators should maintain a sense of mission to cybersecurity, keep vigilant against cyberattacks and incidents, and make continuous efforts to strengthen the systems.

Governments should also make tremendous efforts to protect their critical infrastructure by establishing mandatory security requirements for critical infrastructure, ensuring owners and operators comply with these requirements, and providing security advice as needed. In addition, governments should be transparent about security matters and promptly share threat information with the critical infrastructure operators.

Government organizations, security companies, and manufacturers have different capabilities and specialties. It is, therefore, necessary to create an institutional cooperation mechanism (such as a public-private critical infrastructure security council and a joint cyber response team) so stakeholders' unique capabilities can be integrated at the national level. Each country should also build trust with international partners and actively share information and intelligence. This cooperation will allow like-minded countries not only to detect, prevent, and investigate attacks in a timely manner, but also to build a framework for international collaboration in which they can work together to improve cybersecurity and resilience,

84. "ENTSOE-E Transmission System Map," ENTSO-E (website), January 1, 2019, https://www.entsoe.eu/data/map/; and "Europe Pipelines Map," Theodora (website), March 31, 2017, https://www.theodora.com/pipelines/europe_oil_gas_and_products_pipelines.html.

85. ENISA, *Communication Network Dependencies*, 23–24.

determine attribution for cyberattacks, and take harmonized actions against threat actors who perpetrate them.