# Addressing the Security Challenges of Information Technology / Operational Technology Integration

by John Wang, P.Eng.

July 2026

ospe.on.ca

ONTARIO SOCIETY OF PROFESSIONAL ENGINEERS

# Acknowledgements

This report was developed through the collaborative efforts of dedicated members of Ontario's engineering community. OSPE gratefully acknowledges the contributions of the following individuals:

## Author

John Wang, P.Eng.

## Reviewers

Jeanette Chau

Suyash Khasnobish

Roy Marra, MBA, C.Dir., CGEIT

Stevan Ostojic

Nyron Samaroo

Eram Sayed

Vincent Travaglini, P.Eng.

# Table of Contents



## Tables and Figures

# 1. Executive Summary

The integration of **Information Technology (IT)** and **Operational Technology (OT)** systems is transforming industrial operations, enabling advanced functionality, remote monitoring, and efficiency gains. However, this convergence significantly expands the attack surface, creating new cybersecurity risks. Recent incidents demonstrate that compromises in IT environments can cascade into OT systems, causing severe operational disruptions.

The **Canadian Centre for Cyber Security** warns that IT/OT integration is a critical threat vector, with nation-state actors and cybercriminals increasingly targeting OT assets, particularly within **Critical Infrastructure (CI)**. Emerging trends such as cybercrime-as-a-service and ransomware amplify these risks. In response, Canada is advancing legislation through the **Critical Cyber Systems Protection Act**, which will mandate cybersecurity programs and incident reporting for designated sectors.

This paper outlines best practices for mitigating IT/OT integration cybersecurity risks across the system lifecycle—from requirements and design to operations and decommissioning. Key recommendations include:

- Embedding cybersecurity requirements in all phases of the system development lifecycle
- Implementing robust network segmentation, multi-factor authentication, and centralized logging
- Securing supply chains and maintaining a robust vulnerability management program
- Preparing for post-quantum cryptography challenges

Proactive measures are essential to safeguard safety, reliability, and business continuity in an increasingly interconnected environment.

# 2. Introduction

## 2.1 Background

**Operational Technology (OT)** encompasses hardware and software that monitor and control physical devices, processes, and infrastructure in industrial environments such as manufacturing, energy, transportation, and utilities.

Common OT systems include:

- Programmable Logic Controllers (PLCs)
- Supervisory Control and Data Acquisition (SCADA) systems
- Distributed Control Systems (DCS)
- Building Management Systems (BMS)
- Computer Numeric Controller (CNC) machines and smart instrumentation
- Industrial Internet of Things (IIOT)
- Biomedical Instrumentation
- Power generation systems
- Water and Wastewater Management Systems

OT is a cornerstone of Canada’s infrastructure, powering automation and control systems across energy, water, manufacturing, resource extraction, transportation, healthcare, and municipal services.

**Information Technology (IT)** uses computer systems, networks, and software to manage and process data. These are typically business applications and IT equipment, such as:

- Financial systems
- Human resources systems
- Customer Relationship Management (CRM) systems
- Social media applications
- Desktop productivity tools (e.g. word processing, spreadsheet, presentation software)
- Computer servers
- Laptop computers
- Cell phones

### 2.1.1 Traditional Setups

IT and OT infrastructures are typically air-gapped—physically separated with no direct communication. These infrastructures operate in separate worlds—physically and organizationally.

The following table lists the differences from an organizational perspective. (1) (2)

| | Operational Technology | Information Technology |
|---|---|---|
| Organizational Reach | **Focused reach:** OT systems are designed, implemented and operated by functional groups specific to that OT system. (e.g. the lifecycle of a manufacturing system is managed by the manufacturing department). Typically, each OT system impacts only the business group. | **Broad reach:** Practically everyone in the organization would use some sort of IT system (e.g. electronic mail, organizational intranet). |
| Organizational Impact | **Critical Impact:** OT systems are typically critical systems because they directly support the purpose of the organization. (e.g. a manufacturing system for a manufacturing company). Also, such systems control physical devices, which have direct health and safety impacts. | **Supporting Role:** Unless the organization is in the information economy (e.g. financial services, social media, digital matching services (such as Uber, Airbnb)), IT systems play a supporting role and are not considered the most critical system in the organization. |
| Management Structure | **Business:** The senior manager for the relevant business unit oversees the relevant OT system. (e.g. VP of Manufacturing oversees the manufacturing system) | **IT:** The Chief Information Officer is typically in charge of IT. |
| Equipment Scope | **OT Systems:** Electronic equipment that does not run on general-purpose operating systems (e.g. Microsoft Windows, Linux). These include CNC, SCADA, DCS, etc. OT applications that run on general-purpose operating systems that support OT systems are often maintained by the OT department. Sometimes the underlying operating system is also maintained by the OT department, but not to the same standards as those within IT. | **IT Systems:** Traditional systems that support the organization, such as employee workstations, cell phones, finance and human resource servers and applications, as well as the underlying computer network infrastructure. |

| | | |
|---|---|---|
| Personal Background and Training | **Engineers:** Typically, engineers are involved in the design and management of the implementation and operations of OT systems. (e.g. Industrial engineer for a manufacturing plant or a mining engineer for a mining operation). | **Non-Engineers:** Generally, people in IT are not engineers. The majority come from computer science, though a minority have computer engineering backgrounds or have self-trained to become IT personnel. |
| Information Security | **Outside of:** The information security department's mandate often does not cover OT. | **Embedded:** The information security department is typically within the IT department. |
| Knowledge Transfer Between Industries | **Difficult:** Due to different types of equipment and the unique regulations of each industry, OT knowledge and OT security are more difficult to transfer between industries. It is not easy for an expert on car manufacturing equipment to then become an expert on medical equipment. | **Easy:** IT and IT security knowledge in one industry is easily transferable to another industry.<br>For example, an expert on financial reporting systems used in car manufacturing can easily transfer that knowledge to using a financial reporting system for a hospital. |

**Table 1:** Organizational Differences Between IT and OT Groups

Distinct organizational backgrounds lead to differing characteristics in OT and IT systems.

| | **Operational Technology** | **Information Technology** |
|---|---|---|
| Design and Implementation Emphasis | **Safety & Reliability:** Focuses on safety, reliability ("uptime") and process integrity. | **Confidentiality & Integrity:** Focus on providing a convenient user interface, protecting privacy and confidentiality, and ensuring data integrity.<br>Uptime is less important except when the organization's main purpose is in the information economy. |
| Network Protocol | **OT Specific:** Each OT industry uses its own industry or proprietary network protocols. | **TCP/IP:** Over time, network protocols gravitated to Transmission Control Protocol/Internet Protocol (TCP/IP). |
| Connectivity to the Internet | **Isolated:** Traditionally, OT systems are not connected to the Internet. | **Connected:** Since IT systems use TCP/IP, often they are accessible to the Internet or reside on the Internet. |
| Cybersecurity | **Afterthought:** Historically, cybersecurity was not considered when OT equipment was manufactured or OT systems were designed. | **Incorporated:** Historically, the focus of cybersecurity has been to protect IT systems. Information security is now less of an afterthought and is built into the design of IT equipment and IT system designs. |

| | | |
|---|---|---|
| Authentication / Authorization / Auditing | **Built-in or No Authentication:** In the OT environment, there is greater variation in how authentication is done. Some can authenticate to a central authentication server. In others, the authentication function is built within the OT system and cannot integrate with a central authentication server. In other OT systems, there is no authentication capability, or authentication uses vendor-supplied credentials that cannot be changed.<br><br>Often, the ability to create custom roles with custom fine-grain authorization is limited within OT systems.<br><br>Generally, OT systems do not generate security logs, and it is uncommon for OT systems to send their logs directly into a Security Information and Event Management system. | **External Authentication:** In most IT applications, authentication of the application and the underlying operating system is executed on a dedicated authentication server. This provides capabilities such as single sign-on and multi-factor authentication.<br><br>Most IT systems use role-based access control to provide coarse and fine-grained authorization to precisely enforce least privilege.<br><br>It is common for meaningful authentication logs to be integrated into a Security Information and Event Management system. |
| Cryptography | **Inconsistent:** Due to concerns about resource overhead and lack of computational power, cryptography is often not enabled or not present for fear that it may negatively affect the performance of the OT system. | **Expected:** Any IT system that is expected to transmit, process, or store confidential data or data integrity is of concern and will have cryptographic capabilities. |
| Patches and Updates | **Rarely:** Patches and updates are rarely, if ever, done. The philosophy is “if it is running, don’t change it.” The effort to patch or update is significantly more for OT than for IT since testing must be more rigorous due to potential human safety or direct impact on business operations if the patch or update causes unintentional side effects. | **Regular:** IT systems are constantly being updated with new features and functionalities. Updates and upgrades are continually done, often monthly. For example, Microsoft operating system patches. |
| Equipment Lifetime | **Decades:** Often, OT systems last many decades.<br><br>Examples of typical lifespan by industry:<br>• Industrial environments (e.g., manufacturing, utilities): 15–30 years<br>• Transportation and infrastructure: Often 20+ years<br>• Energy sector: Can exceed 30 years due to regulatory and safety constraints | **Years:** A ten-year-old IT system is considered out-of-date. Vendor support is much shorter than for OT systems. For example, Microsoft supports 5 years of mainstream support and then another 5 years of extended support for a total of ten years. |

**Table 2:** Differences between IT and OT Systems

## 2.2 Purpose

This paper explores cybersecurity risks in IT/OT integration. This paper will provide industry standards and best practices for addressing such risks.

## 2.3 Scope and Limitations

This paper does not focus on any specific industry or system. This paper is based on previous literature and the experience of the writers. Though there are standards and regulations discussed in this paper, it does not represent, nor list all standards or regulations related to IT and OT. The focus of this paper is on the Canadian experience, but that does not mean all regulations, notices, and standards from Canadian governments or industries are fully covered by this paper. Readers should use this paper as a starting point for further research on designing and implementing integrated IT/OT systems.

# 3. Problem Statement

## 3.1 Convergence Trend

Over time, OT systems have gained additional functionality.

- OT systems can now connection to billing systems so that services provided through OT systems may be billed by service usage.
- Performance monitoring data can now be fed to a centralized monitoring system so that trends across multiple systems can be tracked, compared and correlated. The collected OT data can be used to create and validate predictive operational management models, and monitor the safety, effectiveness and efficiency of the OT system. The volume of OT data required to conduct such analysis is often more than the data storage capacity of the OT system. By offloading the computing resources for analysis to IT systems, it preserves the stability and performance of the OT system.
- Remote device configurations and maintenance are efficient when staff are not required to travel and be physically present. Dedicated connections, such as dial-up telephone lines, are being replaced by Internet-based **Virtual Private Networks (VPN)** to streamline the architecture and reduce costs.
- There are now connections between manufacturing systems and design systems to shorten the time from design to manufacturing. For example, **Computer-Aided Design (CAD)** allows an engineer to design a three-dimensional model of the object that is to be manufactured. **Computer-Aided Manufacturing (CAM)** converts the model to a language (often G-Code) that the target **Computer Numerical Control (CNC)** can understand. The machine instructions are uploaded from the CAD/CAM workstation (IT device) into the CNC (OT device).

OT systems are becoming more intelligent and integrated with IT, creating greater organizational value. As a result, OT systems are also using TCP/IP networking protocol, the same standard protocol used by the Internet and IT systems. Interconnection with IT systems and, at times, the Internet, significantly expands OT's attack surface. When OT systems were within their siloed environment, an attacker had to be within the OT environment to attack the system. This often meant that the attacker had to be in the physical location of the OT system, which may be in remote locations or in physically secure facilities.

IT systems, by their nature, are ubiquitous and exist wherever there are knowledge workers who use a laptop or a smartphone. The interconnective nature of IT systems provides convenience for users to access IT resources from anywhere within the organization. It also means that if any system within the IT network is compromised, an attacker can use the compromised system to launch attacks on other systems within the network. When OT systems are integrated with IT, an attacker has an even larger selection of targets to attack.

# 4. Findings

## 4.1 Centre for Cyber Security Cyber Threat Bulletins

The 2020 **Canadian Centre for Cyber Security Cyber Threat Bulletin** advised that:

"We assess that the digital transformation of Operational Technology (OT)—the process of infusing OT with technology derived from the Information Technology (IT) domain—is almost certainly providing cyber threat actors with new opportunities to access and disrupt OT systems by exploiting the increased computing power and connectivity of OT devices. We judge that this almost certainly includes the OT systems in Canada's critical infrastructure (CI)." (3)

**Metasploit** and **Cobalt Strike** are widely used penetration testing tools by both ethical hackers and malicious actors. (4) Metasploit includes modules specifically designed to penetrate OT systems. (5) OT-specific modules enable attackers to exploit systems more efficiently.

## 4.2 Examples of Compromised OT Systems Through IT

The following is an example of an infamous attack on OT systems.

### 4.2.1 2017 National Health Service (NHS) England

**National Health Service England** is England's publicly funded healthcare system. It provides healthcare services through **General Practitioners (GPs)**, hospitals, dentists, pharmacies, and mental health service agencies to all of England's residents. (6)

The 2017 NHS ransomware attack was part of the global **WannaCry** outbreak, which exploited a known vulnerability in **Microsoft Windows** systems. Based on publicly available literature, the following are the most likely steps that led to the compromise of medical devices within the NHS.

1. **Reconnaissance:** NHS was not specifically targeted. Attackers used **EternalBlue** to scan for vulnerable systems exposed to the Internet. EternalBlue is an exploit code developed by the **United States Government National Security Agency (NSA)** (7) along with other exploit codes, such as **DoublePulsar** (8), as part of its cyberwarfare tool kit. The code was leaked by an entity naming itself the **Shadow Brokers** and was used by the developers of WannaCry. Security vendor **Symantec** attributed WannaCry to the **Lazarus Group**, (9) a North Korean government-backed hacking group. (10)
2. **Initial Access:** The initial attack on the NHS happened on Friday, May 12, 2017. (11) At NHS, IT systems, but not medical devices, were exposed to the Internet. Using automated software, the attacker was looking for port 445, typically used for **Server Message Block (SMB)** protocol, a protocol used for file sharing. The attacker then fingerprinted the operating system version by sending specific SMB network packets and analyzed the response, looking to identify unpatched **Windows XP, 7, or 8** systems. (12) As part of the WannaCry package, the attacker used the EternalBlue exploit (CVE-2017-0143 (13) to CVE-2017-0148 (14)) to initiate a buffer overflow attack to allow it to execute remote code on the vulnerable machine. EternalBlue injects a shellcode (a small piece of software code used as the payload in the exploitation of software vulnerabilities) that enables the attacker to use the IP address of the machine to directly communicate with the SMB protocol, allowing it to spread the malware to other vulnerable systems.
3. **Implant backdoor:** Packaged within EternalBlue is DoublePulsar. DoublePulsar is injected deep into the operating system memory of the exploited system. DoublePulsar creates a backdoor into the infected system, allowing the ransomware payload to be transferred from other infected systems to the target infected system. (15)

4. **Execution:** As such, the WannaCry payload was executed. The payload cryptographically encrypted files on the system and generated a ransom demand for payment in bitcoins. (16)
5. **Local Persistence:** WannaCry ran a Windows service (mssecsvc2.0) (17) and placed binaries on the disk of the infected system so that it would automatically restart if the system was rebooted.
6. **Lateral Movement:** WannaCry is a malware worm, meaning that it self-replicates and spreads across computer networks without human interaction. Within the NHS, once WannaCry established an initial beachhead within the NHS's internal network, it automatically and very quickly sought out and exploited other vulnerable systems. These included medical devices such as infusion pumps, electrocardiogram (EKG) monitors, and medical imaging equipment running on vulnerable Windows 7, Windows 2008, and Windows Mobile operating systems. (18) NHS reported that 1220 pieces of diagnostic equipment had been infected, representing 1% of the NHS's equipment. (19) Additional diagnostic equipment was disconnected during the attack to prevent further infection.
7. **Trigger Kill-Switch:** While reverse engineering WannaCry, **Marcus Hutchins**, a security researcher from **Malwaretech**, discovered that WannaCry would reach out to the internet to query the existence of the domain www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com. (20) This unregistered domain name was hard-coded into the malware. If the domain did not exist, WannaCry would continue to spread. After he registered the domain, WannaCry stopped spreading everywhere, including at the NHS. (21)
8. **Ransomware payment:** No NHS organization paid the ransom, since, during the incident, standing advice not to pay was re-circulated by the **National Cyber Security Centre (NCSC)**, the British government's lead authority on cybersecurity. This advice was repeated by **NHS Digital**.

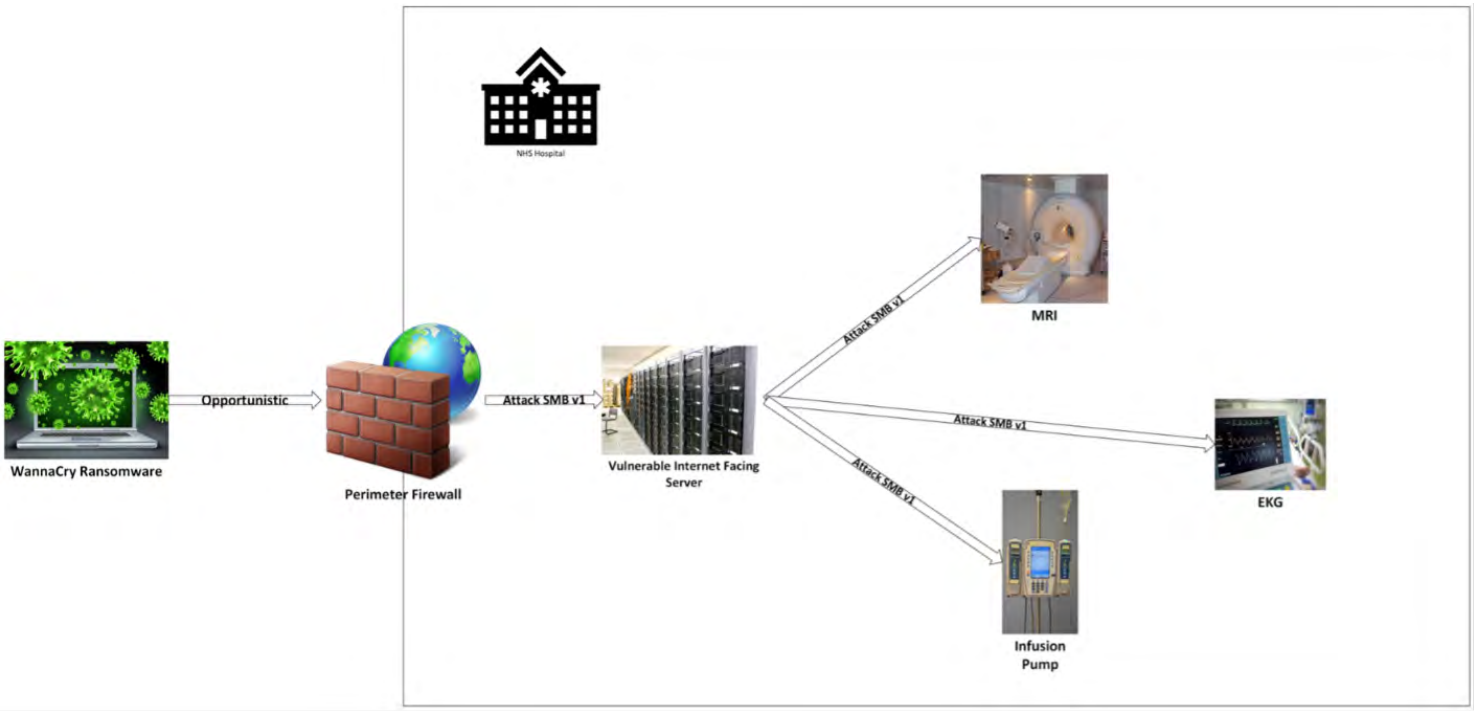


**Figure 1:** WannaCry Attack on NHS

The vulnerabilities at the NHS exposed by the WannaCry ransomware attack were: (22)

- "None of the 80 NHS organizations affected by WannaCry had applied the Microsoft update patch advised by NHS Digital's CareCERT bulletin on 25 April 2017 (two weeks before NHS was attacked), following the receipt of intelligence of a specific threat from British Telecom (BT) on 24 April 2017.
- Whether organizations had patched their systems or not, taking action to increase the security of their network firewalls facing the NHS's N3 network would have guarded organizations against infection.

- This was an attack using a specific Microsoft Windows vulnerability, not an attack on unsupported software. Most NHS devices infected were running the supported, but unpatched, Microsoft Windows 7 operating system. Unsupported devices (those on XP) were in the minority of infected devices, and the number of these devices has decreased in the last 18 months (from the time of the attack) from 18% to 1.8% in January 2018.
- Healthcare is a complex environment with many connected systems. Some critical medical devices/ equipment still use Microsoft XP software supplied by third parties and were affected, including, for example, MRI scanners and blood test analysis devices. This meant that, in some cases, even if a specific diagnostic device was working normally, the software being used to access it, for example, to view X-rays or access blood test results, may not have been available because it was on an infected device or one that had been quarantined because it operated using unsupported software.
- During the incident, national bodies worked together to coordinate advice and support NHS organizations in restoring services and addressing vulnerabilities to the malware attack. NHS England instituted its major incident protocol and coordinated the response through the same team that would deal with any other national major incident. This created a robust framework through which to manage the incident. Lessons have been learned about how a cyber incident differs from other types of major incidents."

WannaCry ransomware impacted the NHS in the following manner:

- The attack led to disruption in one-third of hospital trusts (groups of hospitals and clinics) in England. NHS England data shows that at least 80 out of 236 trusts were affected, with 34 infected and locked out of devices (of which 27 were acute trusts [general hospital services]), and 46 not infected but reporting disruption. A further 603 primary care and other NHS organizations were infected by WannaCry, including 8% of general practitioner practices (595 out of 7,454). During the incident, devices in an additional 21 NHS organizations made calls to the WannaCry 'kill switch'. Whilst this may indicate the presence of infected devices within those organizations, it may also have been the result of routine cybersecurity maintenance activities.
- As part of its incident response, the NHS enacted its "mutual aid" processes in some parts of the country. This meant that where one **Accident and Emergency (A&E)** could no longer take patients, nearby A&Es stepped up to take their demand. During the incident, some patients from five hospitals travelled further for emergency treatment than normal.
- 1.2 % (6,912) of first appointments were cancelled and re-arranged between May 12 and 18, 2017. NHS England's **Emergency Preparedness, Resilience and Response (EPRR)** review identified at least 139 patients who had an urgent appointment for potential cancer that was cancelled, representing approximately 0.4% of urgent cancer referrals.
- The disruption to secondary care had a knock-on effect for primary care, for example in getting access to test results. Third-party systems were also impacted, for example, **DocMan** (an electronic document management system). This impacted the electronic flow of clinical information from secondary care to primary care services.
- During and after the attack, evening and weekend clinics in general practitioner practices were impacted due to the lack of availability of electronic patient records and clinical systems. NHS England did not collect data during the incident on how many GP appointments were cancelled or how many ambulances and patients were diverted from the accident and emergency departments that were unable to treat patients.

### 4.2.2 Other IT / OT Compromise Examples

Other notable examples of OT systems exploited by cyberattacks are:

- **Stuxnet** (2010): Malware installed on infected USB drives were able to jump an air-gapped network to infect **Siemens Step7 Programmable Logic Controllers (PLCs)** used to control uranium enrichment

centrifuges as part of the Iranian government's nuclear program. The payload sent false telemetry to the PLC, thus preventing uranium enrichment from proceeding properly. This was the first known malware specifically designed to target OT systems on a mass scale. (23)

- **Cyberattacks on the Ukrainian Power Grid** (2015, 2016, 2022):
  - » In 2015, attackers gained remote access to IT systems and pivoted their attack to remotely open electrical substation circuit breakers, thus disrupting electrical service to over 200,000 customers. (24)
  - » In 2016, attackers used **Industroyer** malware, which was designed to communicate over IEC 60870-5-104 (IEC 104), a telecontrol protocol used in energy distribution systems for SCADA applications. This enabled communication between control centers and substations over TCP/IP networks. Attackers used this malware to disrupt **Industrial Control Systems (ICS)** within power substations. (25) (26)
  - » In 2022, attackers used an updated version of the Industroyer malware to conduct attacks similar to the attack in 2016. (27) (28)
- **Triton / Trisis** (2017): In 2017, a cyberattack used the **Triton** malware to attack a petrochemical plant in Saudi Arabia. The malware targeted **Schneider Electric Triconex Safety Instrumented Systems (SIS)**. This system acted as the plant's last line of defence by returning processes to safe levels or shutting processes down by triggering shutoff valves and pressure release mechanisms. The malware was designed to disable or tamper with the SIS. The malware used other software to make other parts of the facility malfunction. Fortunately, flaws in the code accidentally triggered the SIS on several occasions, resulting in shutting the plant down and forcing an investigation. During the investigation, the malware was discovered. If the malware had successfully executed, it could have caused the release of toxic hydrogen sulphide gas or caused explosions, putting lives at risk both at the facility and in the surrounding area. Investigations indicated that attackers had penetrated the corporate IT system in 2014 and were able to bypass poorly configured internal firewalls to enter the plant network. This was the first malware designed to put lives at risk. (29)

## 4.3 Canadian Government Threat Assessment

Though all these examples involved systems outside of Canada, the Canadian government has warned that Canada is not immune to cyber threats affecting OT systems. In its 2025-2026 **National Cyber Threat Assessment**, (30) it warned Canadians of the following:

- Russia's cyber threat activities are supported by a network of state and non-state cyber actors, including an ever-shifting group of Russia-nexus cybercriminals, hacktivists, and "hackers-for-hire" who are likely motivated by a mix of patriotism, profit, or opportunism. This hybrid strategy, which provides Russia with deniability, appears to have been emulated by other states, creating a more complex cyber threat environment for Canada. In February 2023, **Pro-Russia Non-State (PRNS)** cyber groups participated in a cyber campaign attempting to sabotage critical infrastructure in countries aiding Ukraine, including Canada. Russian cyber threat actors are very likely targeting the Canadian government, military, private sector, and critical infrastructure networks as part of Russia's foreign and military intelligence collection operations. Although PRNS cyber threat activity against Canada has primarily consisted of **Distributed Denial of Service (DDoS)** attacks and website defacements, some PRNS actors have attempted to compromise OT systems within critical infrastructure in North America and Europe with the intent to disrupt those systems. This activity opportunistically targets internet-accessible devices and exploits basic vulnerabilities, such as insecure remote access software or the use of default passwords. For example, in January 2024, a PRNS group claimed responsibility for the overflow of water storage tanks at water facilities in Texas. The group reportedly posted a video of the compromise and manipulation of control systems at each facility on a public forum. The **Government of Canada** assesses that PRNS actors will likely attempt to disrupt vulnerable internet-connected OT systems within Canadian critical infrastructure when the opportunity arises. PRNS cyber threat activity

against OT may cause systems to malfunction, leading to damage or destruction of those systems and possible harm to public safety.

- Iran has taken advantage of its back-and-forth cyber confrontation with Israel to improve its cyber espionage and offensive cyber capabilities and hone its information campaigns, which it is now almost certainly deploying against targets in the West. While it is unlikely that Canada is, at present, a priority target of Iran's cyber program, Iranian cyber threat actors likely have access to computer networks in Canada, including critical infrastructure. Iranian cyber threat actors have performed denial of service attacks, attempted to manipulate industrial control systems, and accessed government and private networks to encrypt, wipe, and leak data. Iran has developed a network of hacktivist personas and social media channels that exploit these disruptive events to spread the regime's messages and influence the target society, while keeping Tehran's official involvement ambiguous and deniable.
- **Democratic People's Republic of Korea (DPRK)**'s commitment to cybercriminal statecraft presents a persistent and well-resourced cybercrime threat (such as ransomware and cryptocurrency theft) to individuals and organizations in Canada across a broad range of industries and sectors of the economy.
- **People's Republic of China (PRC)** is very likely integrating offensive cyber operations into its military planning to gain an advantage during a potential conflict with the United States. PRC state-sponsored cyber threat actors, tracked as **Volt Typhoon**, are seeking to pre-position within U.S. critical infrastructure networks for disruptive or destructive cyberattacks in the event of a major crisis or conflict with the U.S. According to U.S. officials, the PRC's operation is designed to slow the U.S. military's response and to sow societal panic. The direct threat to Canada's critical infrastructure from PRC state-sponsored cyber threat actors is likely lower than that to U.S. infrastructure. While the focus of future PRC cyber warfare operations will likely be concentrated on the U.S., disruptive or destructive cyber threat activity against integrated North American critical infrastructure, such as pipelines, power grids, and rail lines, would likely affect Canada as well due to cross-border interoperability and interdependence.
- The **Cybercrime-as-a-Service (CaaS)** business model allows attackers with limited technical capabilities to conduct sophisticated attacks and has led to tremendous growth in the cybercrime business. With CaaS, specialized threat actors sell stolen and leaked data and ready-to-use malicious tools to other cybercriminals online, enabling their illicit activities. 2023 was a record-breaking year for ransomware. According to some estimates, the global number of ransomware incidents rose 74% in 2023 compared with 2022, and global ransom payments reached a record of $1 billion USD. By one estimate, the average ransom paid in Canada in 2023 was $1.13 million CAD, an increase of almost 150% in two years. We judge that the ransomware threat will almost certainly continue to grow in the next two years unless significant disruptions to the ransomware ecosystem occur. We assess that ransomware actors are almost certainly opportunistic and do not target specific industries. Ransomware is almost certainly the top cybercrime threat facing Canada's critical infrastructure because it can immobilize critical business operations, destroy or damage important business data, and reveal sensitive information. In addition to the financial losses associated with system repairs and operational disruptions, ransomware attacks can disrupt critical services that put victims' physical safety and emotional well-being in jeopardy. According to cybersecurity reports, victims in 2023 were becoming less likely to pay ransom demands. We judge that the perceived opportunities to earn high profits, combined with victims' reduced willingness to pay, have almost certainly encouraged more technically sophisticated ransomware groups to elevate their extortion techniques and hire skilled affiliates capable of targeting critical infrastructure entities to extract larger ransom payouts. This is called "big game hunting," and we judge that it is the primary strategy used by many of the most prolific ransomware groups impacting Canada. This is in alignment with a 2020 Canadian Centre for Cyber Security Cyber Threat Bulletin, which advised the following.

"We judge that cybercriminals are almost certainly improving their capabilities and are very likely to attempt to target high-value Canadian organizations with large OT assets, including those in [Critical

Infrastructure] CI, in search of larger ransom payments and valuable data. Cybercriminals are also increasingly likely to directly access, map, and exploit OT for extortion with custom ransomware."

The Canadian Centre for Cyber Security Cyber Threat Bulletin also advised that:

"Software supply chain compromises are very likely an active, increasing threat to OT security, and that activity affecting popular software vendors highlights the potential aggregate impact of a critical vulnerability in widely-used OT products." (3)

# 5. Recommendations

## 5.1 Organizational

As mentioned previously, since IT and OT groups have different mandates and cultures, they should remain as separate groups. From an organizational structure perspective, consider the following:

**Clear Accountability for Cybersecurity:** If the cybersecurity group is outside of IT and OT, then consider having a single person within the organization who is accountable for both IT and OT security programs, typically the chief security officer. If IT and OT have their own security departments within IT and OT groups, then typically there will be separate people who are accountable for IT and OT security programs. Regardless of whether it is one or two people, it must be clear who is accountable for the security programs of which set of technologies. (31) (32)

**Regular Communications Between IT and OT Groups:** IT and OT groups should have regular meetings to discuss subjects such as the strategic direction of each group, new technologies being considered, how the groups can leverage new technology, and how integration of existing IT and OT systems can be improved. Cybersecurity must be part of such meetings to identify and provide security guidance. The business group that the OT system supports must also participate to ensure that IT, OT, and cybersecurity align with business strategy. (32)

**Implement Enterprise Risk Management (ERM):** Implement ERM within the organization so that various types of risks can be consistently measured. Clearly specifying the organization's risk appetite and using a common risk scoring model will allow the organization to compare risks within IT and OT so that they can be properly prioritized and their mitigation appropriately resourced. Consider leveraging well established ERM frameworks such as **Committee of Sponsoring Organizations (COSO)** (33) or **ISO 31000**. (34) (35) (36)

If there is a pattern for a series of tactical risks (e.g. risks related to specific vulnerabilities within specific IT or OT systems), and the pattern of behaviour or practice can have a significant negative impact on the organization, then the tactical risks should be consolidated into a strategic risk. The strategic risk must be presented to an enterprise risk management committee for review and gain support for an enterprise solution. For example, insurance companies often state that **Multi-Factor Authentication (MFA)** must be implemented on all systems. If MFA is not implemented, then the insurance company will not honour any cyber-insurance claims. Through a series of risk assessments on various IT and OT systems, it is determined that MFA is not consistently implemented. The ERM committee must then, based on the information gathered from the risk assessments, determine whether it is worthwhile to replace systems that don't support MFA, update other systems to enable MFA, and establish how quickly systems can be updated to comply to the insurance company's requirement to implement MFA. The ERM committee must decide whether the organization will self-insure during the period of non-compliance while MFA is universally implemented or decide that it is not feasible for the foreseeable future to purchase cyber-insurance due to the MFA eligibility requirement. A scenario like the above happened to the **City of Hamilton**. The city's insurance provider in this case denied a claim to recuperate expenses for a 2024 ransomware attack due to non-compliance. (37)

Regardless of risks related to IT, OT, or their integration, risk management must be structured into at least three lines of defence. To enforce proper segregation of duty, the primary responsibility of each line is with different groups. (38) (39)

1. **First Line, Operations:** This refers to the managers and staff who operate the IT / OT systems. They are responsible for identifying risks and implementing appropriate controls in accordance with the organization's approved set of policies and procedures. For proper separation of duty, the people and tools that implement, operate, and conduct performance monitoring of IT and OT systems must be separate from those that monitor the security behaviour of IT and OT systems. In other words, the people and tools within a **Security Operations Centre (SOC)** must be separated from those in the IT or OT operations centres. This separation of duty helps protect the organization from both external and internal threat actors.
2. **Second Line, Risk Management and Compliance:** This group establishes the relevant risk management frameworks, policies, procedures, and tools to allow those in the first line to effectively manage risk. They regularly conduct compliance monitoring to assess the consistency and effectiveness of the controls implemented by the operations team. They help operations identify and manage risk.
3. **Third Line, Internal Audit:** Internal audits provide independent assurance to the organization's board of directors and senior management. Their primary function is to provide oversight of operations and risk management by determining the effectiveness of governance, risk management, and internal controls.
4. **Additional Lines of Defence:** External bodies such as external auditors, industry regulators, and security certification assessors can provide important additional governance and control when there is effective coordination with the aforementioned lines of defence. This is especially important where organizations are publicly traded or in a regulated industry. (40)

**Cybersecurity Policies and Standards:** Where possible, a consistent set of cybersecurity policies and standards must be developed by the risk management team and socialized with appropriate groups within IT, OT, and business units that OT supports. Standards must take into consideration the challenges and limitations of OT systems. Cybersecurity best practice may differ between IT and OT industries. As such, organizational cybersecurity standards may differ between IT and OT systems. The organization's cybersecurity standards must comply with industry regulations and cybersecurity insurance requirements (if the organization has taken out cyber insurance) and take into consideration the maturity of its cybersecurity program. Policies and standards must be reviewed and updated periodically so that they continue to align with business goals, IT/OT direction and budget constraints and address findings from security assessments and audits. Policies must also comply with changing regulations and continually improve the maturity of the organization's cybersecurity program.

**Security Incident Response Planning:** Develop a cybersecurity incident response plan that integrates responses for IT and OT incidents. When documenting the plan, take into consideration how to respond to incidents that affect both IT and OT systems. When testing the plan, invite representatives from cybersecurity, IT and OT to test threat scenarios that affect both types of systems. (32) If a breach is of a criminal nature, ensure that the incident plan includes discussions with the organization's legal counsel, and breach coach (41) on when law enforcement should be involved. (42)

**Basic IT and OT Cybersecurity Training:** In addition to basic cybersecurity awareness training for all employees, ensure that personnel who design, implement, maintain, operate, or secure IT/OT as part of their regular duties receive IT and/or OT specific cybersecurity training that is relevant to their job function, at least annually. (32) Since understanding security requires understanding the technology of the system that is being secured, cross training IT, OT, and cybersecurity staff on the fundamentals of how IT and OT systems function will provide deeper insight into how to protect such systems.

**Implement Industry Specific Security Standards:** In addition to well recognized information security standards such as ISO 27002 (43) there are industry specific security standards. Ensure that your organization complies with your industry's security standards. The following are examples of security standards and guidance within various industries. Check with your industry regulator on what security standards apply to your organization.

1. **Critical Infrastructure:**
    - "Principles of Operational Technology Cyber Security" describe six principles that guide the creation and maintenance of a safe, secure critical infrastructure OT environment. It was authored by the **Australian Signals Directorate (ASD)'s Australian Cyber Security Centre (ACSC)** and co-sealed by various countries' cybersecurity government bodies including the **Canadian Centre for Cyber Security**. The six principles are: (44)
        i. Safety is paramount
        ii. Knowledge of the business is crucial
        iii. OT data is extremely valuable and needs to be protected
        iv. Segment and segregate OT from all other networks
        v. The supply chain must be secure
        vi. People are essential for OT cybersecurity
    - The Canadian government has established the **Cross-Sector Cyber Security Readiness Goals (CRGs)** to provide Canadian organizations with voluntary guidance to improve critical infrastructure cybersecurity. It consists of 36 foundational goals to strengthen cybersecurity. These goals apply to both IT and OT systems and are not sector specific. (32)
    - The **United States Department of Energy** has created the Cybersecurity **Capability Maturity Model (C2M2)** to help organizations evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both IT and OT assets and environments. The free model was developed with asset owners and operators in the electricity, oil, and natural gas industries, but can be used for organizations in all sectors. (45)
    - **International Society of Automation (ISA) / International Electrotechnical Commission (IEC) 62443** is a series of standards for ensuring the safety, integrity, reliability, and security of automation and control systems. It was developed by ISA and submitted to IEC for global adoption. The series addresses the security of **Industrial Automation and Control Systems (IACS)** throughout their lifecycles, which applies to all automation and control systems. The ISA Security Compliance Institute (ISCI), a wholly owned ISA certification consortium certifies suppliers of control systems that their products comply with the ISA/IEC 62443 family of cybersecurity standards. (46)
    - The United States **National Institute of Standards and Technology (NIST) Special Publication 800-82 Guide to Operational Technology (OT) Security** provides guidance on how to secure operational technology while addressing unique performance, reliability, and safety requirements. (47) The current version (version 3) follows the NIST Cybersecurity Framework. (48)
2. **Energy & Utilities:**
    - The **North American Electric Reliability Corporation (NERC)** has developed the **Critical Infrastructure Protection (CIP)** (49) series of standards which is a baseline set of cybersecurity controls. In Ontario, the **Independent Electricity System Operator (IESO)** is responsible for compliance monitoring and enforcement (50) with the rollout of scheduled enforcement dates published on their website. (51)
3. **Oil & Gas:**
    - **Canadian Standards Association CSA Z246.1:21** ***Security Management for Petroleum and Natural Gas Industry Systems*** (52) uses risk management to address security issues within the petroleum and natural gas industries.

- The **American Petroleum Institute (API) Standard 1164** ***Pipeline Control Systems Cybersecurity*** provides requirements and guidance for managing cyber risks associated with **Industrial Automation and Control (IAC)** environments. Version 3 of the standard includes new requirements on cybersecurity, and improved risk assessment guideline. (53)

4. **Water & Wastewater:**
   - The United States **Environmental Protection Agency (EPA)** and the **Cybersecurity and Infrastructure Security Agency (CISA)** have developed a set of cybersecurity recommendations to limit the vulnerability of **Human-Machine Interfaces (HMI)** in water and wastewater facilities and secure them against malicious cyber activity. In the absence of adequate cybersecurity controls, unauthorized remote users could exploit human-machine interfaces to view and adjust real-time system settings. These unauthorized adjustments can potentially disrupt the facility's water and/or wastewater treatment process. (54)
   - **America's Water Infrastructure Act (AWIA)** section 2013, as of 2018, requires **Community Water Systems (CWS)** serving more than 3,300 people to prepare or revise their **Risk and Resilience Assessments (RRAs)** and certify to the EPA that this work has been completed. As part of these RRAs, a cybersecurity assessment must be included. The EPA provides a cybersecurity tool kit to facilitate self-assessment. (55)
   - Canada does not have a direct equivalent to AWIA but organizations such as the **Ontario Water Works Association** endorses EPA's cybersecurity tool kit and the **Canadian Cyber Security Readiness Goals Toolkit**. (56)
5. **Transportation:**
   - **Transport Canada** has developed a suite of guidance and tools on cybersecurity for vehicles. These resources can help industry stakeholders develop organizational vehicle cybersecurity strategies. They provide useful information on vehicle cybersecurity threats and best practices for maintaining a strong cybersecurity posture. (57)
   - The **United States Department of Homeland Security** has provided a cybersecurity toolkit for surface transportation operators who have fewer than 1,000 employees. Their website provides a set of resources to guide transportation operators to guard against cybersecurity attacks. (58)
   - The **International Maritime Organization (IMO)** has issued ***Guidelines on Maritime Cyber Risk Management***. The guideline provides high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The IMO encourages that cyber risks be appropriately addressed in existing safety management systems no later than the first annual verification of the company's Document of Compliance after January 1, 2021. (59) The IMO also endorses guidelines from other organizations such as:
     i. Baltic and International Maritime Council (BIMCO)'s Guidelines on Cyber Security Onboard Ships (60)
     ii. Independent Association of Ports and Harbors (IAPH) Cybersecurity Guidelines for Ports and Port Facilities (61)
     iii. IAPH's Cyber Resilience Guidelines for Emerging Technologies in the Maritime Supply Chain (62)
   - The **Radio Technical Commission for Aeronautics (RTCA) DO-326 (A, B)** provides augmented guidance for aircraft certification to handle information security threats to aircraft safety. (63) A similar set of standards is provided by **EUROCAE ED-202A Airworthiness Security Process Specification**. (64) They were developed in tandem and became the sole **Acceptable Means of Compliance (AMC)** for the **Federal Aviation Administration (FAA)** and the **European Union Aviation Safety Agency (EASA)** cybersecurity airworthiness certification. The purpose of the airworthiness security process is to ensure that when there is an unauthorized interaction, the aircraft will always remain in a condition for safe operation. (65)

## 5.2 Infrastructure

As IT and OT are integrated, they can no longer exist in siloed environments. Infrastructure needs to be re-architected to accommodate the new requirements for the two types of systems to communicate.

### 5.2.1 Access Control

**Changing Default Passwords:** While changing default passwords on an organization's existing OT requires significantly more work, organization's should enforce a policy to change default credentials for all new or future devices. This is not only easier to achieve but also reduces potential risk in the future if adversary **Tactics, Techniques, and Procedures (TTPs)** change. (32)

**Unique Credentials:** Unique and separate credentials should be provisioned for accounts to access IT versus OT networks. This prevents attackers from reusing compromised credentials to move laterally between IT and OT networks. (32)

**Phishing-Resistant Multifactor Authentication (MFA):** Within OT environments, enable MFA on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible human-machine interfaces. Phishing-resistant MFA is intended to prevent attackers from stealing or relaying secrets. Examples of phishing-resistant MFA include hardware-based MFA, mobile app-based soft tokens (preferably a push notification with number matching) or emerging technology such as FIDO passkeys. (32) **Any Time-based One-Time Password (TOTP)** delivered by email, short message service, voice-based MFA or authenticator apps, such as **Google Authenticator**, **Authy**, **Microsoft Authenticator**, are not recommended since they are more susceptible to social engineering-based attacks. Authenticator apps such as Microsoft Authenticator can also use push-based notifications with number matching, which is the preferred method of using the app.

**Implement Zero-Trust Network Access (ZTNA) Where Possible:** Many organizations are replacing legacy network based **Virtual Private Networks (VPN)** with ZTNA. This allows for more precise and adaptive access and session control to on-premises and cloud services. (66) ZTNA works well with modern network protocols but often OT applications still need to use traditional VPN technology. (67)

**Privileged Access Management (PAM):** Since access to OT systems is used to conduct privileged activities that affect the performance and safety of the system, strict control needs to be enforced on who, what, and when access into an OT system is permitted. **Information Technology Infrastructure Library (ITIL)** change management should leverage a PAM solution so that any change (regardless of whether it is normal, standard, or emergency) to the OT system is tightly controlled. Access should only be granted to the systems that require change, and only for the duration of the change window. Access must only be granted to identifiable individuals who are authorized to execute the change. Group accounts must not be permitted. When remote access is used to access OT systems, session monitoring should be enabled to record all actions executed on the OT system. This can assist in troubleshooting if the change is not successful or identify unauthorized activity.

**Decide on Single or Multiple Authentication Servers:** Consider separate authentication servers to segregate authentication to IT and OT systems. According to Microsoft, "it's no surprise that domain controllers [authentication servers used in Microsoft environments] are frequently at the center of ransomware operations. Cyber-attackers consistently target them to gain privileged access, move laterally, and rapidly deploy ransomware across an environment. We've seen in more than 78% of human-operated cyberattacks, threat actors successfully breach a domain controller. Additionally, in more than 35% of cases, the primary spreader device—the system responsible for distributing ransomware at scale—is a domain controller, highlighting its crucial role in enabling widespread encryption and operational disruption." (68) If an attacker is able to compromise an authentication server, then the attacker can use the compromised server to further

compromise IT and OT systems if both types of systems authenticate off of the same server. When designing authentication systems, conduct a risk assessment and cost-benefit analysis to determine whether IT and OT accounts should use a single authentication server, or separate authentication servers. Additionally, decide if all OT systems will authenticate off of a single authentication server, or if each OT system will have their own dedicated server. When making such a decision, the organization needs to consider: (69)

- Cost to administrate different servers and additional accounts
- Ability to enforce consistent policies across authentication servers
- Licensing costs
- User experience of having one or more accounts
- Size of blast radius if an authentication server is compromised
- Integration cost to integrate various OT systems into a single authentication server
- Timing of downtime when service work needs to be conducted on an authentication server

### 5.2.2 Network Segmentation

**Network Segmentation:** All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a **Demilitarized Zone (DMZ)**, which is closely monitored, captures network logs, and only allows connections from approved assets. (32) Ensure that firewalls that protect OT environments recognize appropriate OT network protocols so that they can conduct deep inspection of network connections.

**Architecture:** Consider using recognized reference network architecture models for segmenting between IT and OT systems. These models include the **Purdue Model** (70), **American National Standards Institute / International Society of Automation (ANSI/ISA) -95** (71) (also known as **International Electrotechnical Commission (IEC) 62264** (72) ) and **Industrial Internet Consortium (IIC) Industrial Internet of Things Reference Architecture** (73). For example, the ISA-95 model is as follows: (71)

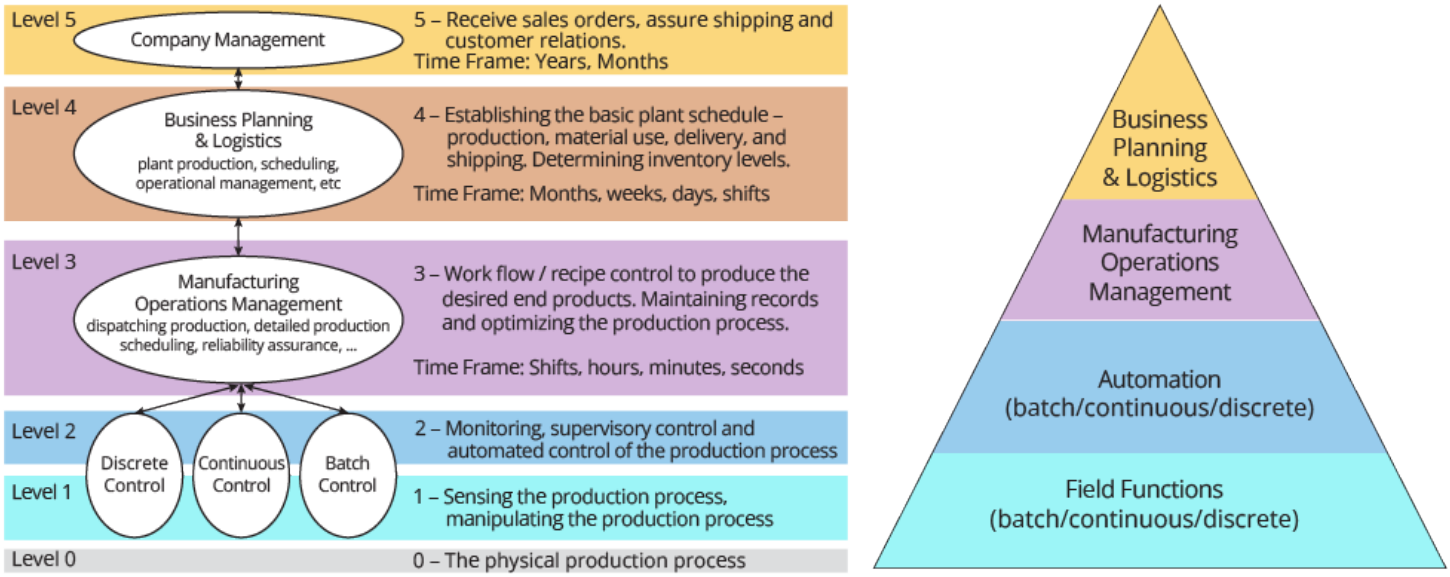


**Figure 2:** ISA-95 model

- **Level 0: Physical Production Processes:** Level 0 describes the physical processes of running a plant. It refers to machinery and other assets in the field or on the floor.
- **Level 1: Sensing and Manipulating the Production Process:** Level 1 describes the collection of data and the manipulation of physical processes. It refers to sensors, smart devices, valves and other devices that sense or affect production.
- **Level 2: Monitoring and Supervising Control:** Level 2 describes the monitoring and supervising of physical processes in the manufacturing environment. It refers to Programmable Logic Controllers (PLCs), Distributed Control Systems (DCSs) and other control devices.
- **Level 3: Manufacturing Operations Management:** Level 3 describes Manufacturing Execution Systems (MES) and other systems such as SCADA that manage manufacturing operations. The ISA-95 standard primarily deals with the interface between levels 3 and 4.
- **Level 4: Business Planning and Logistics:** Level 4 describes all the activities related to running a business. It includes Enterprise Resource Planning (ERP) systems.

**NIST SP 800 -82 Guide to Operational Technology (OT) Security** (47) provides sample network architectures for DCS-Based OT Systems, DCS- and PLC-Based OT with IIoT, and SCADA-Based OT environments.

**Limit OT Connections to Public Internet:** Ensure no OT assets are on the public internet, unless explicitly required for operation. Require that exceptions be justified and documented and that excepted assets have additional protections in place to prevent and detect exploitation attempts (e.g., logging, MFA , mandatory access via proxy or another intermediary). (32) If leveraging cloud services, use recognized architectural frameworks (see above) to ensure proper network segregation.

**Implement a Cyber-Physical Systems (CPS) Protection Platform:** Consider integrating the OT system with a cyber-physical systems protection platform. Such products use knowledge of industrial protocols, operational/production network packets or traffic metadata, and physical process asset behaviour to discover, categorize, map and protect CPS in production or mission-critical environments outside of enterprise IT environments. When deciding which CPS protection platform to acquire, consider reviewing Gartner's Magic Quadrant for this segment. (74)

### 5.2.3 Logging

**Log Collection:** Collect IT and OT logs in a security information and event management system. Correlate the logs to establish what is considered normal traffic between IT and OT systems. Set up alerts when abnormal traffic or user/system behaviour is detected. For OT assets where logs are non-standard or not available, collect network traffic and communications between OT assets and other assets. (32)

### 5.2.4 Documentation

**Asset inventory and Network Topology:** Maintain a regularly updated inventory of all assets within the organization's IT and OT networks. (32) This is a valuable resource for troubleshooting and dealing with security incidents. This information will allow an incident responder to understand the flow of an attack.

**Maintain an Up-to-Date Bill of Materials (BoM):** Have suppliers provide a bill of materials (hardware, software, cryptographic components, cloud services, etc.) for the products and services offered so that any vulnerabilities within the components can be identified. For example, an OT device may be running on an operating system that is no longer supported. In that case, either replace the device with one that runs on a supported operating system or design compensating controls. The ransomware incident at NHS is an example of where a **Software Bill of Materials (SBoM)** would have helped identify vulnerable medical devices. The Canadian Centre for Cyber Security has joined CISA and other international partners in releasing guidance on a shared vision of SBOM for cybersecurity. The guidance aims to inform software producers,

purchasers and operators of the benefits of integrating SBOM generation, analysis, and sharing into security processes and practices. (75)

Information relating to the bill of materials must be maintained in a central location logically linked to its assets. This may be in an asset management system or an ERP system. If the organization is using an **Information Technology Service Management (ITSM)** system and follows the ITIL framework, the ITSM should integrate with the asset management system. Sometimes this is a software module available for the ITSM or ERP so that the configuration items within the **Configuration Management Database (CMDB)** can be properly linked with its BoM within the asset management system or ERP. If, through the ITIL change management process, the BoM changes (for example if an operating system on a server is upgraded), then, the organization should follow ITIL's service asset and configuration management process within the ITSM system to update the configuration items (server) and allow the integration of the two systems to update the BoM (operating system version) within the asset management or ERP system. (76)

**Document Device Configurations:** Maintain accurate documentation, describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management, response, and recovery activities. (32)

**Keep Documentation Secure:** Ensure that all documents related to the design, development and implementation of IT and OT systems are stored and transmitted securely. Access to such documents must be on a need-to-know basis. If such documents are leaked to attackers, they can use the knowledge to identify vulnerabilities and plan an attack.

## 5.3 Systems Development Lifecycle (SDLC)

### 5.3.1 Requirements

**Document Cybersecurity Requirements:** Ensure that not only functional requirements are defined but also availability, safety, privacy and security requirements are defined. Requirements must comply with industry regulations, government mandates, and organizational policies. Document which requirements are mandatory, and which are non-mandatory.

**Prepare for a Post-Quantum World:** Since OT systems typically have long lifespans and upgrading systems is not frequently done, it is important to consider future-proofing these systems. Cryptography enables secure data storage and transmission, as well as ensures authentication credentials remain secure. Quantum computers will break the currently used cryptographic algorithms, like those based on factoring and discrete logarithms. If IT and OT systems continue to use traditional cryptographic algorithms when quantum computing becomes viable, then all such systems will become vulnerable to compromise. Organizations such as NIST are actively developing standards for **Post-Quantum Cryptography (PQC)**. An important note, PQC algorithms are not required to be run on quantum computers but can be run on traditional computers. PQC algorithms are designed to be difficult for both existing conventional computers and projected quantum computers to crack. PQC algorithms use larger key lengths and signatures thus requiring more computing resources than traditional cryptographic algorithms. (77) OT systems typically have fewer computing resources than IT systems and may not have sufficient computing resources to run intensive PQC algorithms. Organizations with OT systems that have long operational lives should adapt PQC into their planning. This would include the following: (78)

1. Maintain an up-to-date cryptographic bill of materials in order to understand what systems are vulnerable in a post-quantum world.
2. Conduct a risk assessment of such systems in a post-quantum situation to determine the likelihood and impact (such as safety) of the system if the confidentiality or integrity of the data within the system is compromised.

3. Based on the outcome of the risk assessment, prioritize systems that need to be transitioned into using PQC.
4. Monitor post-quantum standards development. For example, NIST has released its first three post-quantum encryption standards. (79)
5. As part of the organization's supplier strategy, align with crypto-agile vendors. Request that OT vendors provide their post-quantum product roadmap so that major overhaul of OT systems will not be required when the OT system needs to be upgraded for a post-quantum world.

### 5.3.2 Design

**Incorporate Cybersecurity Requirements into Design:** Ensure that all mandatory availability, safety, privacy and security requirements are incorporated into the design.

**Design Controls to Protect Safety Instrumented Systems (SIS):** SIS are systems that protect humans or the environment by automatically shutting down parts of production processes safely in the event of a hazardous occurrence. Protect SIS from **Denial of Service (DOS)** attacks so that a malicious actor cannot shut down production while having the SIS disabled. Malware such as **Triton** are being developed specifically targeting SIS. (29)

**Protect from Physical Tampering or Vandalism:** Include physical design considerations such as where and how OT systems will be deployed. Decide on what controls will be in place to prevent physical tampering or vandalism. Design how systems will be physically monitored (using cameras and alarms, for example) to detect unauthorized physical access to the systems. Often OT systems are deployed in remote locations (e.g. SCADA) lacking the physical infrastructure to protect such systems. If an attacker can obtain physical access to the system, the attacker may be able to bypass cybersecurity controls, thus compromising the safety of the system. They may also use the compromised system as a launchpad for attacking other systems within the organization.

**Use Robust Cryptographic Algorithms Where Possible:** Design the IT and OT systems to use, at minimum, non-deprecated cryptographic algorithms. To minimize the impact to latency and availability, use encryption where feasible, it is often feasible for OT communications connecting with remote/external assets. (32) Incorporate post-quantum computing plans into the design of the OT system where possible. This may include incorporating **Quantum-Resistant Cryptography (QRC)** into the design if there is vendor support. (80)

### 5.3.3 Development

**Implement Secure Software Development Procedures:** Scan all development code for vulnerabilities and remediate issues promptly. Ensure that any third-party application libraries are scanned for vulnerable code and replaced with secure versions of those libraries before they are used by custom developed code.

### 5.3.4 Testing

**Test in a Non-Production Environment:** Though it may not always be feasible to create a full test environment, test as much as possible in a non-production environment. This includes security testing, such as configuration reviews, vulnerability scans and penetration tests of IT and OT components. Testing should include testing all IT and OT accounts to ensure that the principle of least privilege is enforced, meaning that users, programs and systems, should only have the minimum access required to perform their role. When using vulnerability scanning tools or penetration testing tools, ensure that the testing tools have the appropriate OT testing modules that support the specific OT system being tested. In the test environment, consider:

- Conducting Denial of Service testing to determine if the OT system is vulnerable to such attacks.

- Testing systems in manual mode as part of incident response planning. If IT and OT systems need to be disconnected or OT systems need to be taken off the network, can the OT system continue to operate? (81)

### 5.3.5 Deployment

**Conduct a Configuration Review:** Review the configuration of production systems to confirm that they are properly hardened and that least privilege is enforced.

**Prohibit the Connection of Unauthorized Devices:** Establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices, or establish procedures for granting access through approved exceptions. (32)

**Conduct a Physical Security Review:** Review the physical configurations and environments where IT and OT systems are deployed to ensure that they cannot be physically tampered with or vandalized. Consider exercising a physical penetration test to test the adequacy of physical and procedural controls that prevent unauthorized people from entering restricted areas where IT and OT systems are deployed. Ensure that physical security detection and alerting systems are properly deployed and monitored to alert for unauthorized entry.

**Change Management:** Implement formal change management processes that require approval before new hardware, firmware, or software/software version is installed or deployed. Ensure that processes include testing to validate the safety and security of the system before the change ticket is closed. (32) Ensure that there is a backout plan in case the change is unsuccessful. Consider using **Information Technology Infrastructure Library (ITIL)** as a framework for implementing formal change management. (82)

### 5.3.6 Operations and Maintenance

**Vulnerability and Patch Management:** Use a risk-based approach to determine what OT systems can and should be updated or patched. Monitor threat feeds that notify of attacks on vendors' IT or OT systems to determine whether there have been any supply chain compromises. Review patch documentation to determine whether the patch applies to the organization's environment. Maintain an up-to-date software and component bill of materials to determine whether the patch applies to software or components within the organization's environment. Review the severity level of the identified vulnerability, the critical nature of the OT system, whether the system contains confidential information and whether the vulnerability is being actively exploited to determine the level of risk and the urgency in which the OT system needs to be patched. If patching is not urgent, consider incorporating patching as part of the OT system's regular maintenance cycle. (83) For assets where patching is not possible or may substantially compromise availability or safety, apply and record compensating controls (e.g., segmentation, monitoring). Carefully select and configure automated vulnerability detection tools as they can scan systems aggressively. These tools may cause OT devices to behave erratically, stop working/crash, restart, or need manual intervention to revert to an operational state. (32)

**Backup IT and OT Systems:** Back up on a regular cadence all systems that are necessary for operation. Ensure stored information for OT assets includes at a minimum: (32)

- configurations
- roles
- PLC logic
- engineering drawings
- tools

Backing up this type of data should be a task in the change ticket within an ITIL change management process. The frequency of backing up business data must comply with the business' Recovery Point Objective (RPO).

Follow the industry practice of 3-2-1. (84)

- **3 Copies:** In addition to the original version, keep three copies in case there is a copy failure or a failure of the copying system.
- **2 Different Types of Storage Media:** Store the copies on two different types of media (hard drive, solid state drive, cloud storage, tape, etc.) so that if one medium fails, there is another medium.
- **1 Offline:** Keep one copy offline, off-site, and immutable. This copy can be used if an attacker has encrypted all the online data including online backups. This copy can also be used if a disaster has occurred destroying your production data centre.

Encrypt backup data, so if the data is exfiltrated or the storage media is stolen, it will take time for the attacker to decrypt the data. This will provide the organization with time to notify stakeholders and change cryptographic keys and authentication credentials before the attacker has an opportunity to exploit the information. The strength of encryption should be determined by the length of time the confidentiality of the data remains a concern. The longer the time required, the greater the strength is required. If the length of time is indeterminate, consider using post-quantum cryptography.

**Third-Party Validation of Cybersecurity Control Effectiveness:** Third parties with demonstrated expertise in IT and/or OT cybersecurity should regularly validate the effectiveness and coverage of an organization's cybersecurity defences. Conduct these exercises annually to include activities such as penetration tests, bug bounties, incident simulations, or table-top exercises. Include both unannounced and announced tests. (32)

### 5.3.7 Decommission

**Decommissioning Systems:** The decommissioning of any IT or OT system must follow a formal change management process (see ITIL change management (82)). Tasks in the change ticket should include:

- Ensure that data is in a format that is readable without the use of the decommissioned system. If the data is confidential, ensure that the archived data is encrypted with an encryption algorithm that is expected not to be deprecated over its records retention period.
- Take the system offline.
- Set the system back to factory default settings.
- Disable any accounts within the authentication server that are no longer needed.
- Update firewall rules or SIEM rules to account for the removal of the asset.
- Securely wipe or destroy storage components that contain confidential data.
- Update the asset inventory to indicate that the system has been decommissioned. Specify within the records management system or asset inventory system where archived data is stored.
- Update architectural documentation when systems have been decommissioned.
- If the system or data storage component is to be disposed, ensure that a certificate of destruction is received from the IT asset disposition provider.

## 6. Critical Cyber Systems Protection Act (CCSPA)

As of June 15, 2026, Bill C-8 has received Royal Asset. (85) Within the bill is the **Critical Cyber Systems Protection Act (CCSPA)** (86). The Act applies to telecommunications, interprovincial and international pipelines and power lines, nuclear energy, federally regulated transportation systems, and financial services sectors. The Act requires designated operators in such industries to:

- Establish, implement, and maintain a cybersecurity program within 90 days of designation, notify the appropriate regulator that such a program has been established, and provide the appropriate regulator with the program details. The program should:
  - » Identify, manage and mitigate risks including risks related to third-party product service providers and supply chains.
  - » Protect critical cyber systems from compromise.
  - » Detect cybersecurity incidents affecting critical systems.
  - » Minimize the impact of any cybersecurity incident.
- Conduct and file annual reviews of their cybersecurity program and notify regulators of any material changes.
- Report cybersecurity incidents to the **Communications Security Establishment** and notify their regulators within 72 hours (or an earlier timeframe if prescribed).
- Comply with confidential cybersecurity directions issued by the federal government.
- Maintain all cybersecurity records in Canada, in a prescribed manner and location.

The Act would grant industry regulators the power to verify compliance, including the authority to conduct audits, issue compliance orders, and enter premises. Enforcement of the Act can include,

- **Administrative Penalties:** Monetary penalties, compliance agreements, and personal liability for directors and officers. Regulators can issue **Administrative Monetary Penalties (AMPs)** up to $15 million per violation per day, for organizations and $1 million per violation, per day, for individuals.
- **Criminal Offences:** Regulators can initiate regulatory proceedings leading to fines. Directors and officers of designated operators could be held personally liable if they were complicit in committing a serious violation which can lead to possible imprisonment for up to five years. (87)

The Act outlines high-level requirements for establishing and maintaining cybersecurity programs but lacks details. Details are expected in future regulations. This would result in operators compiling a comprehensive inventory of their cybersecurity systems and assessing their criticality. The lack of detailed requirements is compounded by the government's authority to issue binding cybersecurity directives without consulting operators on feasibility, cost, or service continuity impacts. (88) Therefore organizations may risk receiving such directives because they were not clear on the requirements.

## 7. Conclusion

IT/OT integration offers significant operational benefits but introduces complex cybersecurity challenges. Expanded attack surfaces and increasingly sophisticated threat actors demand a holistic, lifecycle-based approach to security. Organizations must integrate cybersecurity into design, operations, and governance frameworks while aligning with emerging regulations such as the Critical Cyber Systems Protection Act.

Success requires collaboration between IT and OT teams, adherence to industry standards, and continual risk management. By implementing the recommendations outlined in this paper, ranging from network segmentation and secure authentication to supply chain integrity and post-quantum readiness, organizations can strengthen resilience against evolving threats. Ultimately, safeguarding IT/OT integration is not only a technical imperative but a strategic necessity for protecting critical infrastructure and ensuring public safety.

## 8. Glossary of Terms

**Access Control**
Policies and mechanisms that regulate who can view or use resources in IT and OT environments.

**Air-Gapped**
Systems or networks are air-gapped when they are physically isolated from external connections, including the Internet.

**Authentication Server**
A system that verifies user identities and credentials before granting access to IT or OT resources.

**Bill of Materials (BoM)**
A detailed list of hardware, software, and components used in a system, essential for identifying vulnerabilities.

**Building Management System (BMS)**
A control system that manages building operations such as HVAC, lighting, and security.

**Cybercrime-as-a-Service (CaaS)**
A business model where cybercriminals sell tools and services to enable attacks by others.

**Cyber-Physical System (CPS) Protection Platform**
Technology that monitors and secures systems combining physical processes with digital control, such as industrial automation.

**Distributed Control System (DCS)**
An OT system that uses decentralized controllers to manage industrial processes.

**Demilitarized Zone (DMZ)**
A network segment that acts as a buffer between internal systems and external networks, reducing exposure to threats.

**Denial of Service (DoS)**
An attack that disrupts system availability by overwhelming resources or exploiting vulnerabilities.

**Operational Technology (OT)**
Hardware and software systems that monitor and control physical devices and processes in industrial environments.

**Industrial Internet of Things (IIoT)**
Network of interconnected sensors, instruments, and other devices networked together with computers' industrial applications, including manufacturing and energy management.

**Information Technology (IT)**
Systems and processes for managing data, including business applications, servers, and networks.

**Programmable Logic Controller (PLC)**
A specialized computer used to automate industrial processes.

**Recovery Point Objective (RPO)**
The RPO defines the maximum amount of data that can be lost during an outage.

**Safety Instrumented System (SIS)**
A system designed to automatically shut down processes safely during hazardous conditions.

**Security Information and Event Management (SIEM)**
A platform that aggregates and analyzes logs from IT and OT systems for threat detection and response.

**Supervisory Control and Data Acquisition (SCADA)**
An OT system for monitoring and controlling industrial processes remotely.

**Zero-Trust Network Access (ZTNA)**
A security model that enforces strict identity verification for every user and device attempting to access resources.

## 8.1 Standards and Frameworks

**API STD 1164**
American Petroleum Institute Standard for Pipeline Control Systems Cybersecurity, providing requirements and guidance for managing cyber risk in industrial automation and control environments.

**Cybersecurity Capability Maturity Model (C2M2)**
Developed by the U.S. Department of Energy to help organizations evaluate and improve cybersecurity capabilities for IT and OT systems.

**Critical Cyber Systems Protection Act (CCSPA)**
Canadian legislation mandating cybersecurity programs and incident reporting for designated critical infrastructure sectors.

**Committee of Sponsoring Organizations Enterprise Risk Management (COSO ERM)**
A widely recognized framework for managing organizational risk, including cybersecurity.

**IEC 62264**
This International Electrotechnical Commission standard describes the manufacturing operations management domain (Level 3) and its activities, and the interface content and associated transactions within Level 3 and between Level 3 and Level 4. This description enables integration between the manufacturing operations and control domain (Levels 3, 2, 1) and the enterprise domain (Level 4).

**IEC 62443**
International standard for securing industrial automation and control systems throughout their lifecycle.

**IMO Guidelines**
International Maritime Organization guidelines for managing maritime cyber risk within safety management systems.

**ISA-95**
International Society of Automation provides a set of standards aimed at integrating logistics systems with manufacturing control systems. It organizes technology and business processes into layers defined by activities taking place, and it outlines how an enterprise can set up an interface to communicate among these layers.

**ISO 27002**
International standard providing best practices for information security controls, including cybersecurity and privacy protection.

**ISO 31000**
International standard for risk management principles and guidelines.

**Information Technology Infrastructure Library (ITIL)**
A framework for IT service management, including processes for change management and incident response.

**North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)**
Standards for securing critical infrastructure in the electricity sector.

**NIST Cybersecurity Framework (CSF)**
Developed by the U.S. National Institute of Standards and Technology to provide a risk-based approach to managing cybersecurity.

**NIST SP 800-82**
Guide to Operational Technology (OT) Security, addressing unique performance, reliability, and safety requirements.

**RTCA DO-326 / EUROCAE ED-202A**
Standards for cybersecurity in aviation, ensuring airworthiness and safe operation under cyber threats.

## 8.2 Emerging Technologies

**Post-Quantum Cryptography (PQC)**
Encryption methods designed to withstand attacks from quantum computers.

**Quantum-Resistant Cryptography (QRC)**
Algorithms intended to remain secure against quantum computing threats.

## 9. References


1. **Voster, Wam.** Implement a Four-Phase Approach to CPS Security. *Gartner*. [Online] July 15, 2025. https://www.gartner.com/document-reader/document/6722834. ID G00834154.

2. **Kristian Steenstrup, Earl Perkins.** As IT and OT Converge, IT and Engineers Should Learn From Each Other. *Gartner*. [Online] April 19, 2024. https://www.gartner.com/document-reader/document/3979664. ID G00450675.

3. **Canadian Centre for Cyber Security.** Cyber threat bulletin: Cyber threat to operational technology. *Canadian Centre for Cyber Security*. [Online] December 16, 2021. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-operational-technology. ISBN 978-0-660-41268-9 .

4. **Sheridan, Kelly.** Cobalt Strike & Metasploit Tools Were Attacker Favorites in 2020. *Dark Reading*. [Online] January 7, 2021. https://www.darkreading.com/cyber-risk/cobalt-strike-metasploit-tools-were-attacker-favorites-in-2020.

5. **SCADAhacker.com.** Metasploit Modules for SCADA-related Vulnerabilities. *SCADAhacker.com*. [Online] September 10, 2012. https://scadahacker.com/resources/msf-scada.html.

6. **National Health Service.** NHS Services. *National Health Service (NHS)*. [Online] https://www.nhs.uk/nhs-services/.

7. **Timberg, Ellen Nakashima and Craig.** NSA officials worried about the day its potent hacking tool would get loose. Then it did. *The Washington Post*. [Online] May 16, 2017. https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

8. **Sidagni, Michelangelo.** The Shadow Brokers-Leaked Equation Group's Hacking Tools: A Lab-Demo Analysis. *NopSec*. [Online] April 26, 2017. https://www.nopsec.com/blog/the-shadow-brokers-leaked-equation-groups-hacking-tools-a-lab-demo-analysis/.

9. **Johnson, A L.** WannaCry: Ransomware attacks show strong links to Lazarus group . *Broadcom*. [Online] May 22, 2017. *https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b2b00f1b-e553-47df-920d-f79281a80269&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments*.

10. **Patairya, Dilip Kumar.** Who is the Lazarus Group? The hackers behind billion-dollar heists. *COINTELEGRAPH*. [Online] March 2, 2025. https://cointelegraph.com/learn/articles/lazarus-group-hackers-behind-billion-dollar-heists.

11. **National Audit Office.** Investigation: WannaCry cyber attack and the NHS. *National Audit Office*. [Online] October 27, 2017. *https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/*.

12. **Langde, Rohit.** WannaCry Ransomware: A Detailed Analysis of the Attack. *TechSpective*. [Online] September 26, 2017. *https://techspective.net/2017/09/26/wannacry-ransomware-detailed-analysis-attack/*.

13. **National Vulnerability Database.** CVE-2017-0143 Detail. *National Vulnerability Database*. [Online] March 3, 2017. *https://nvd.nist.gov/vuln/detail/CVE-2017-0143. CVE-2017-0143*.

14. —. CVE-2017-0148 Detail. *National Vulnerability Database*. [Online] March 16, 2017. https://nvd.nist.gov/vuln/detail/CVE-2017-0148. CVE-2017-0148.

15. **bhassani.** DoublePulsar Backdoor. *DeepWiki*. [Online] https://deepwiki.com/bhassani/EternalBlueC/4-doublepulsar-backdoor.

16. **British Broadcasting Corporation.** Massive ransomware infection hits computers in 99 countries. *British Broadcasting Corporation*. [Online] May 13, 2017. https://www.bbc.com/news/technology-39901382.

17. **Clark, Zammis.** The worm that spreads WanaCrypt0r. *Malwarebytes Labs*. [Online] May 12, 2017. https://www.malwarebytes.com/blog/news/2017/05/the-worm-that-spreads-wanacrypt0r.

18. **Jeff Hussey.** Two Years Later, Windows XP Devices Can Still Make The Health Care Industry Wannacry. *Forbes*. [Online] August 2, 2019. https://www.forbes.com/councils/forbestechcouncil/2019/08/02/two-years-later-windows-xp-devices-can-still-make-the-health-care-industry-wannacry/.

19. **General, Comptroller and Auditor.** Investigation: WannaCry cyber attack and the NHS. *National Audit Office*. [Online] April 25, 2018. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

20. **National Health Services Digital.** WannaCry Ransomware Using SMB Vulnerability. *NHS Digital*. [Online] May 12, 2017. https://digital.nhs.uk/cyber-alerts/2017/cc-1411. Threat ID: CC-1411.

21. **Hutchins, Marcus.** How to Accidentally Stop a Global Cyber Attacks. *Malware Tech*. [Online] May 13, 2017. https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html.

22. **Smart, William.** Lessons learned review of the WannaCry Ransomware Cyber Attack. *National Health Services*. [Online] February 1, 2018. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.

23. **Fruhlinger, Josh.** Stuxnet explained: The first known cyberweapon. *CSO*. [Online] August 31, 2022. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.

24. **MITRE ATT&CK.** 2015 Ukraine Electric Power Attack. *MITRE ATT&CK*. [Online] December 18, 2024. https://attack.mitre.org/campaigns/C0028/. ID: C0028.

25. —. 2016 Ukraine Electric Power Attack. *MITRE ATT&CK*. [Online] April 16, 2025. https://attack.mitre.org/campaigns/C0025/. ID: C0025.

26. —. Industroyer. *MITRE ATT&CK*. [Online] April 04, 2024. https://attack.mitre.org/software/S0604/.

27. —. 2022 Ukraine Electric Power Attack. *MITRE ATT&CK*. [Online] March 27, 2024. https://attack.mitre.org/campaigns/C0034/. ID: C0034.

28. **Rob Wright.** Industroyer2: How Ukraine avoided another blackout attack. *TechTarget*. [Online] August 10, 2022. https://www.techtarget.com/searchsecurity/news/252523694/Industroyer2-How-Ukraine-avoided-another-blackout-attack.

29. **Giles, Martin.** Triton is the world's most murderous malware, and it's spreading. *MIT Technology Review*. [Online] March 5, 2019. https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/.

30. **Canadian Centre for Cyber Security.** National Cyber Threat Assessment 2025-2026. *Government of Canada*. [Online] October 30, 2024. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026.

31. **Kristian Steenstrup, Jo-Ann Clynch.** How CIOs Are Approaching IT/OT Alignment and Integration. *Gartner*. [Online] February 8, 2024. https://www.gartner.com/document-reader/document/5181863. ID G00807419.

32. **Canadian Centre for Cyber Security.** Cross-Sector Cyber Security Readiness Goals Toolkit. *Canadian Centre for Cyber Security*. [Online] October 29, 2024. https://www.cyber.gc.ca/en/cyber-security-readiness/cross-sector-cyber-security-readiness-goals-toolkit. D96-121/2024E-PDF.

33. **Committee of Sponsoring Organizations of the Treadway Commission.** Enterprise Risk Management. *Committee of Sponsoring Organizations*. [Online] 2017. https://www.coso.org/guidance-erm.

34. **International Standards Organization.** ISO 31000:2018 Risk management — Guidelines. *International Standards Organization*. [Online] 2018. https://www.iso.org/standard/65694.html. ISO 31000:2018.

35. **Johnson and Wailes University.** 12 Benefits of Enterprise Risk Management. *JWO Online*. [Online] January 10, 2023. https://online.jwu.edu/blog/benefits-enterprise-risk-management/.

36. **Gopal, Deepti.** How to Harmonize Cybersecurity Risk and Enterprise Risk Management. *Gartner*. [Online] July 28, 2025. https://www.gartner.com/document-reader/document/6775834. ID G00821135.

37. **Beattie, Samantha.** Insurance won't cover $5M in City of Hamilton claims for cyberattack, citing lack of log-in security. *CBC News*. [Online] Canadian Broadcasting Corporations, July 31, 2025. https://www.cbc.ca/news/canada/hamilton/cybersecurity-breach-1.7597713.

38. The Institute of Internal Auditors. The IIA's Three Lines Model An Update of the Three Lines of Defense. *The Institute of Internal Auditors*. [Online] July 2020. https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf.

39. **The Compliance Digest.** Explaining the Three Lines of Defence (3LOD) Model. *The Compliance Digest*. [Online] https://thecompliancedigest.com/explaining-the-three-lines-of-defence-3lod-model/.

40. **The Institute of Internal Auditors.** IIA Posistion Paper: The Three Lines of Defense in Effective Risk Management and Control. *Institute of Risk Management*. [Online] January 2013. https://www.theirm.org/media/5487/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf.

41. **Insurance Training Centre.** What is a Breach Coach? *Insurance Training Centre*. [Online] https://insurancetrainingcenter.com/resource/what-is-a-breach-coach/.

42. **RCMP.** National Cybercrime Coordination Centre. *Royal Canadian Mounted Police*. [Online] November 3, 2025. https://rcmp.ca/en/federal-policing/cybercrime/national-cybercrime-coordination-centre.

43. **International Standards Organization.** ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. *International Standards Organization*. [Online] 2022. https://www.iso.org/standard/75652.html. ISO/IEC 27002:2022.

44. **Austrailian Signals Directorate.** Principles of operational technology cyber security. *Austrailian Signals Directorate*. [Online] October 2, 2024. https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/principles-operational-technology-cyber-security.

45. **US Department of Energy.** Cybersecurity Capability Maturity Model (C2M2). *US Department of Energy*. [Online] June 2022. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

46. **International Society of Automation.** ISA/IEC 62443 Series of Standards. *International Society of Automation*. [Online] February 2, 2025. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. ISA/IEC 62443.

47. **Computer Security Resource Center.** NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security. *National Institute of Standards and Technology*. [Online] September 2023. https://csrc.nist.gov/pubs/sp/800/82/r3/final. NIST SP 800-82 Rev. 3.

48. **National Institute of Standards and Technology.** The NIST Cybersecurity Framework (CSF) 2.0. *National Institute of Standards and Technology*. [Online] February 26, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

49. **North American Electric Reliability Corporation.** CIP - Critical Infrastructure Protection. *North American Electric Reliability Corporation*. [Online] https://www.nerc.com/standards/reliability-standards/cip.

50. **Independent Electricity System Operator.** Reliability Standards Framework. *Independent Electricity System Operator*. [Online] https://www.ieso.ca/Sector-Participants/System-Reliability/Reliability-Standards-Framework.

51. **Independent Electricity System Operator.** Ontario Enforcement Dates for NERC Reliability Standards and NPCC Criteria. *Independent Electricity System Operator*. [Online] https://www.ieso.ca/Sector-Participants/System-Reliability/Enforcement-Dates.

52. **Canadian Standards Organization.** CSA Z246.1:21 Security management for petroleum and natural gas industry systems. *Canadian Standards Organization Group*. [Online] 2021. https://www.csagroup.org/store/product/2428754/. SKU: 2428754.

53. **American Petroleum Institute.** API STD 1164: Pipeline Control Systems Cybersecurity. *American Petroleum Institute*. [Online] August 1, 2021. https://www.apiwebstore.org/standards/1164. API STD 1164.

54. **United States Environmental Protection Agency**. https://www.epa.gov/system/files/documents/2024-12/joint-factsheet-epa-cisa-internet-exposed-human-machine-interfaces-508c.pdf. *United States Environmental Protection Agency*. [Online] September 29, 2025. https://www.epa.gov/system/files/documents/2024-12/joint-factsheet-epa-cisa-internet-exposed-human-machine-interfaces-508c.pdf.

55. —. Cybersecurity Assessments. *United States Environmental Protection Agency*. [Online] https://www.epa.gov/cyberwater/cybersecurity-assessments.

56. **Ontario Water Works Association**. Water and Wastewater Cybersecurity CISA Toolkit - Canadian Centre for CyberSecurity. *Ontario Water Works Association*. [Online] https://owwa.ca/news-post/water-and-wastewater-cybersecurity-cisa-toolkit-canadian-centre-for-cybersecurity/.

57. **Transport Canada.** Vehicle cyber security. *Transport Canada*. [Online] August 6, 2021. https://tc.canada.ca/en/road-transportation/innovative-technologies/connected-automated-vehicles/vehicle-cyber-security.

58. **US Department of Homeland Security.** Surface Transportation Cybersecurity Toolkit. *US Department of Homeland Security*. [Online] https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit.

59. **International Maritime Organization.** Maritime cyber risk. *International Maritime Organization*. [Online] April 4, 2025. https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx. MSC-FAL.1/Circ.3/Rev.3.

60. **Baltic and International Maritime Council.** THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

version 5. *Baltic and International Maritime Council*. [Online] November 14, 2024. https://www.bimco.org/media/s4ddrsfe/2024-11-14-guidelines_on_cyber_security-v5-final.pdf.

61. **Independent Association of Ports and Harbors.** IAPH Cybersecurity Guidelines for Ports and Port Facilities version 1.0. *International Maritime Organization*. [Online] July 2, 2021. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/IAPH%20Cybersecurity%20Guidelines%20for%20Ports%20and%20Port%20Facilities%20v1.pdf.

62. **Independent Association of Ports and Harbors.** CYBER RESILIENCE GUIDELINES FOR EMERGING TECHNOLOGIES. *International Maritime Organization*. [Online] https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/IAPH%20Cyber%20resilience%20guidelines%20for%20emerging%20technologies%20in%20the%20maritime%20supply%20chain%20ENG.pdf.

63. **Radio Technical Commission for Aeronautics.** Introducing RTCA's Security Standards and Training Partnership. *Radio Technical Commission for Aeronautics*. [Online] https://www.rtca.org/security/.

64. **EUROCAE.** ED-202A | Airworthiness Security Process Specification. *EUROCAE*. [Online] May 2014. https://www.eurocae.net/product/ed-202a-airworthiness-security-process-specification/.

65. **LDRA.** DO-326B/ED-202A Trusted Aerospace Cybersecurity Framework Guide. *LDRA*. [Online] https://ldra.com/aerospace-security-framework/.

66. **Gartner.** What should I know about ZTNA? *Gartner*. [Online] https://www.gartner.com/fast-answer/tech/a3452578-b086-3f14-b0f4-409a9b98a5f2.

67. **Bob Gill, Mohini Dukes.** 5 IT/OT Decisions Necessary for Edge Computing Success. *Gartner*. [Online] September 22, 2023. https://www.gartner.com/document-reader/document/4769631?ref=solrAll&refval=512354900&. ID G00780539.

68. **Rosental, Alon.** How cyberattackers exploit domain controllers using ransomware. *Microsoft Security*. [Online] April 9, 2025. https://www.microsoft.com/en-us/security/blog/2025/04/09/how-cyberattackers-exploit-domain-controllers-using-ransomware/.

69. **Voster, Wam.** Pros and Cons of Using Corporate Active Directory for Your CPS. *Gartner*. [Online] April 28, 2025. https://www.gartner.com/document-reader/document/6396075. ID G00822991.

70. **Garton, David.** Purdue Model Framework For Industrial Control Systems & Cybersecurity Segmentation. *US Department of Energy*. [Online] November 12, 2019. https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf. Topic Paper #4-14.

71. ***International Society of Automation.*** ISA-95 Series of Standards: Enterprise-Control System Integration. *ISA Standards*. [Online] https://www.isa.org/standards-and-publications/isa-standards/isa-95-standard.

72. **International Electrotechnical Commission.** IEC 62264-1 IEC 62264-1:2013 Enterprise-control system integration - Part 1: Models and terminology. *International Electrotechnical Commission*. [Online] May 22, 2013. https://webstore.iec.ch/en/publication/6675. IEC 62264-1.

73. **Indusrial Internet Consortium**. The Industrial Internet of Things Volume G1: Reference Architecture Version 1.9. *Indusrial Internet Consortium*. [Online] June 19, 2019. https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf.

74. **Katell Thielemann, Wam Voster, Ruggero Contu.** Magic Quadrant for CPS Protection Platforms. *Gartner*.

[Online] February 12, 2025. https://www.gartner.com/interactive/mq/6171823. ID G00808225.

75. **Canadian Centre for Cyber Security.** Joint guidance on a shared vision of software bill of materials for cyber security. *Canadian Centre for Cyber Security*. [Online] September 3, 2025. https://www.cyber.gc.ca/en/news-events/joint-guidance-shared-vision-software-bill-materials-cyber-security.

76. **Locke, Randal.** 10 Ways Your CMDB Influences ITIL Success. Ivanti. [Online] August 31, 2023. https://www.ivanti.com/blog/cmdb-in-itil.

77. **Palo Alto Networks.** What Is Post-Quantum Cryptography (PQC)? A Complete Guide. *Palo Alto Networks*. [Online] https://www.paloaltonetworks.com/cyberpedia/what-is-post-quantum-cryptography-pqc.

78. **Cybersecurity and Infrastructure Security Agency.** Post-Quantum Considerations for Operational Technology. *Cybersecurity and Infrastructure Security Agency*. [Online] October 2024. https://www.cisa.gov/sites/default/files/2024-10/Post-Quantum%20Considerations%20for%20Operational%20Technology%20%28508%29.pdf.

79. **National Institute of Standards and Technology.** NIST Releases First 3 Finalized Post-Quantum Encryption Standards. *National Institute of Standards and Technology*. [Online] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

80. **Ivezic, Marin.** Upgrading OT Systems to Post Quantum Cryptography (PQC): Challenges and Strategies. *Post Quantum*. [Online] November 7, 2023. https://postquantum.com/post-quantum/ot-pqc-challenges/#protocol-and-hardware-constraints.

81. **Canadian Centre for Cyber Security.** Protect your operational technology. *Canadian Centre for Cyber Security*. [Online] July 2022. https://publications.gc.ca/site/eng/9.912179/publication.html. ISBN 9780660440262.

82. **Kempter, Stefan.** Change Management. *IT Process Maps*. [Online] https://wiki.en.it-processmaps.com/index.php/Change_Management.

83. **Lina Al Dana, Todd Larivee, Chris Saunderson.** How to Balance Patch Management and Operational Resilience. *Gartner*. [Online] July 29, 2025. https://www.gartner.com/document-reader/document/6784934. ID G00828056.

84. **Micron.** What is the 3-2-1 backup rule? *Micron Crutial*. [Online] June 14, 2024. https://www.crucial.com/articles/about-ssd/why-you-should-follow-the-3-2-1-backup-rule.

85. **Amundson, Quinton.** Cyber security Bill C-8 passes second reading. *The Catholic Register*. [Online] October 7, 2025. https://www.catholicregister.org/item/2877-cyber-security-bill-c-8-passes-second-reading.

86. **Government of Canada.** BILL C-8 An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. *Government of Canada*. [Online] June 18, 2025. https://publications.gc.ca/collections/collection_2025/parl/XB451-8-1.pdf.

87. **Leslie Milton, Christopher Ferguson, Paul Burbank, Olivia Elliot.** Bill C-8 Reboots Canada's Cybersecurity Legislation for the Telecommunications Sector and Other Critical Infrastructure. *Fasken*. [Online] October 2, 2025. https://www.fasken.com/en/knowledge/2025/10/bill-c-8.

88. **Hélène Deschamps Marquis, Daniel J. Michaluk, Eric S. Charleston, Matt Saunders, Claire Feltrin.** Bill C-8 revives Canadian cyber security reform: What critical infrastructure sectors need to know. *Borden Ladner*

*Gervais LLP*. [Online] July 28, 2025. https://www.blg.com/en/insights/2025/07/bill-c8-revives-canadian-cyber-security-reform-what-critical-infrastructure-sectors-need-to-know.

## Contact Us

Ontario Society of Professional Engineers
5000 Yonge Street, Suite 701
North York, ON, M2N 7E9
1-866-763-1654
info@ospe.on.ca



ONTARIO SOCIETY OF PROFESSIONAL ENGINEERS