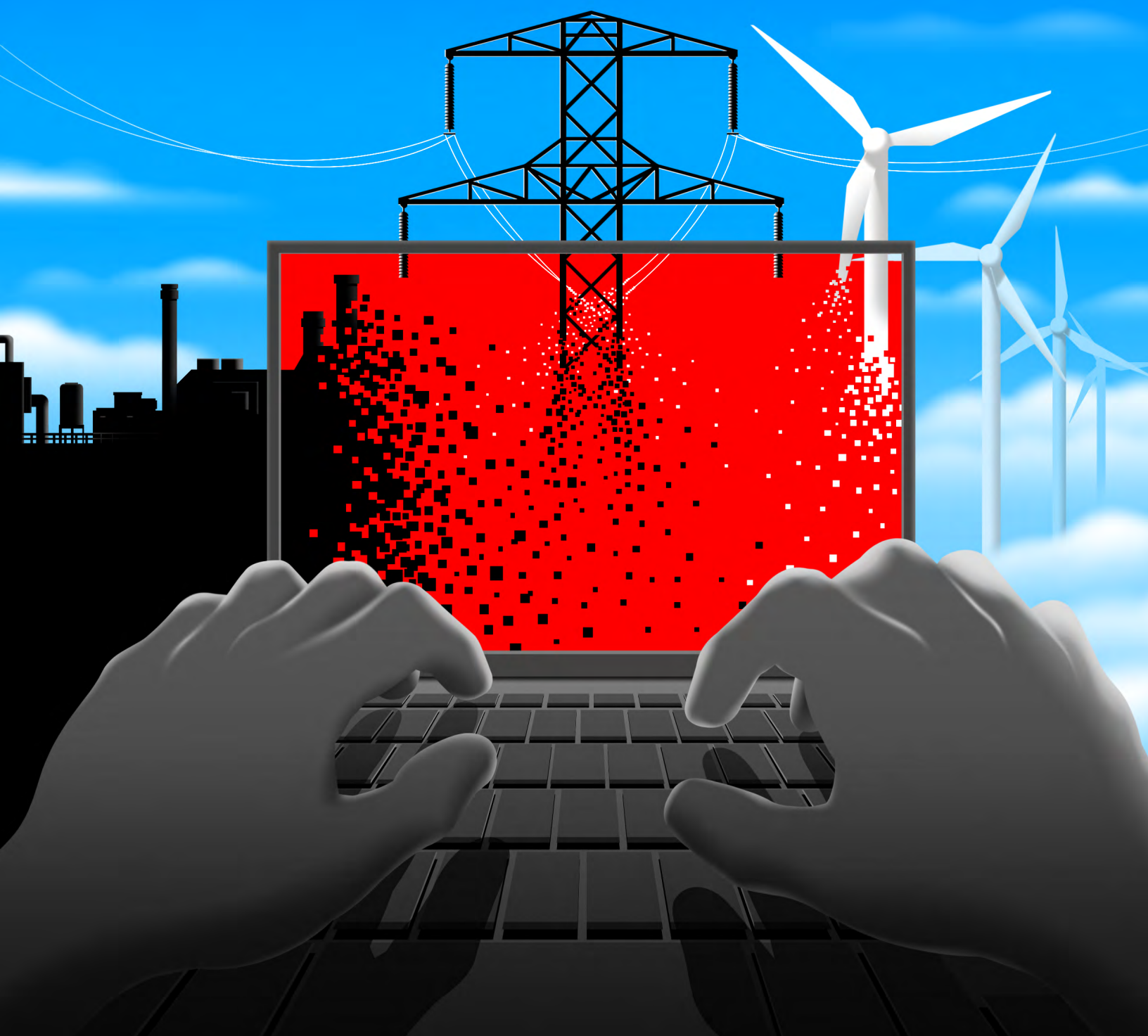


State of OT

Securing Canada's critical infrastructure



Contents & Contributors



Anson Chan

Freelance Illustrator and the artist behind our cover illustration.



Tristan Kim

Director, Cyber Risk, Innovation & Strategy at Kore Solutions and co-author of *Smart Infrastructure, Smarter Threats*.

6



Youssef Jad

CTO and Co-founder of CyVault™ and co-author of *Smart Infrastructure, Smarter Threats*.

6



Enza Alexander

Executive Vice-President and author of *Why Critical Infrastructure Must Prioritize Cybersecurity*.

11



Denrich Sananda

Managing Partner at Arista Cyber and co-author of *From Guidelines to Guardrails*.

15



Sonia Khan

Cybersecurity Consultant at Arista Cyber and co-author of *From Guidelines to Guardrails*.

15



Daly Brown

CEO and co-author of *Defence vs. Commercial: Not So Different When Protecting Critical Assets*.

20



Nick Foubert

CTO and co-author of *Defence vs. Commercial: Not So Different When Protecting Critical Assets*.

20



Sandeep Lota

Global Field CTO at Nozomi Networks and author of *How to Establish a CCSPA-Compliant Cybersecurity Program for Critical Cyber Systems*.

24



Juveria Khan

Founder and author of *Secure Modernization Starts with a Map*.

30

Contents & Contributors



Xage Security and Darktrace present and co-author *Securing Industrial Modernization*.

34



Anton Livaja

CEO and author of *Reproducible Builds and Full-Source Bootstrapping*.

40



Jason Grimbeek

CEO of Iron Spear Information Security and author of *The Evolving Operational Technology (OT) Security Landscape*.

43



François Guay

Founder of the Canadian Cybersecurity Network and author of *The Human Impact of OT Failures*.

49



Ashif Samnani

Cyber Security Principal at MOBIA Technology Innovations and co-author of *Stronger Together: Securing Critical Infrastructure with IT/OT Convergence*.

54



Burt Kim

COO and co-author of *Stronger Together: Securing Critical Infrastructure with IT/OT Convergence*.

54



Rob Labbé

CEO and author of *Why Integrate IT and OT Security?*

59



Francois J. Driessen

COO, CMO and Co-Founder of ADAMnetworks™ and author of *Canada Strong: Rising to the Challenge to secure OT with Zero Trust Connectivity*.

65



Charlie Tsao

Engagement and Community Specialist and editor of *State of OT Report 2025*.



Jen Spinner

Creative director of *State of OT Report 2025*.


Introduction

by François Guay

The Canadian Cybersecurity Network (CCN) is Canada's largest cybersecurity community, with over 45,000 members and a reach of nearly one million professionals, businesses, academics, and government leaders. Our mandate is clear: to increase cybersecurity awareness, grow Canada's cyber economy, and build national resilience. We believe cybersecurity is not just an IT issue, it is a matter of public safety, economic stability, and national security.

This **national** OT report has been authored by **thought leaders** from across Canada, representing a broad spectrum of **industries**, including mining, smart cities, oil and gas, energy, healthcare, and manufacturing.

Together, they offer real-world insights from the front lines of operational technology, where cybersecurity decisions directly impact safety, reliability, and the quality of life Canadians depend on every day.

OT now lies at the core of energy grids, hospitals, transportation systems, and city infrastructure. The risks of inaction are simply too great as cyber threats against OT continue to escalate, bringing with them the potential for real-world harm. This report contributes to a national conversation by spotlighting these risks and advancing practical solutions. By bringing together industry voices, data-driven examples, and actionable insights, CCN continues its mission to make cybersecurity a shared responsibility across Canada. 



Executive Summary

Operational technology (OT) is the backbone of Canada's quality of life. It powers cities, secures healthcare, drives industry, and connects communities from coast to coast to coast. Yet as OT systems converge with IT, they have become one of the most attractive and dangerous targets for cyber criminals, hackers, and nation-states.

The numbers tell the story. In 2024, 73% of reported cyber incidents impacted OT systems, up from 49% the year before. The Canadian Centre for Cyber Security has made it clear that public safety and human lives depend on OT system integrity. Energy providers are now tracking 60 new vulnerabilities in grid networks every single day, while hospitals face ransomware that can delay surgeries, divert ambulances, and endanger patients. The 2024 Black Basta ransomware attack on Ascension Health, which disrupted care for millions, is a stark reminder of what happens when OT is left exposed.

The risks do not stop at hospitals and power plants. From remote mining operations to urban water treatment facilities, OT is everywhere, and so are attackers. The 2025–2026 National Cyber Threat Assessment warns that ransomware and nation-state probing of critical infrastructure are “almost certain” to continue. The convergence of IT and OT means a single phishing email can cascade into an industrial shutdown.

This report explores these risks in depth, sector by sector. It examines how emerging technologies such as AI and quantum computing are reshaping the battlefield and highlights regulatory changes through Bill C-8 and the Critical Cyber Systems Protection Act. Finally, it offers practical steps organizations can take now, embedding security by design, building trust between IT and OT teams, and making resilience a national priority.

The conclusion is unavoidable: resilience starts with readiness. Cybersecurity cannot be bolted on; it must be built in. Protecting OT is not only about securing systems, it is about protecting people, communities, and Canada's future prosperity.

Call to Action

At the Canadian Cybersecurity Network, we believe **Canada's future** depends on how well we protect the systems that protect us. **Safeguarding OT is no longer optional**, it is essential to our economy, our safety, and our sovereignty.

We call on government, industry, and community leaders to act together:

- **Invest in resilience** with modernization and secure-by-design principles.
- **Break down silos** between IT and OT teams to build trust and accelerate response.
- **Share intelligence openly** across sectors, because attackers already do.
- **Develop talent** through training, awareness, and opportunities for the next generation of Canadian cybersecurity leaders.

Canada is at a crossroads. By acting decisively now, we can lead the world in building secure, resilient, and innovative OT systems that safeguard not only our critical infrastructure but the very quality of life Canadians hold dear. ☸



Smart Infrastructure, Smarter Threats: Rethinking OT Security in the Built Environment

By [Tristan Kim](#) and [Youssef Jad](#), Presented by Kore Solutions and CyVault™

A Cautionary Story: Blind Spot in a Glass Tower

At a recent industry roundtable, a CISO at a large Canadian financial institution claimed, “I don’t have OT risk.” But when asked about his daily commute, he described parking in a smart garage, badging through access systems, and taking an elevator to the 25th floor—each powered by OT infrastructure his company either owned or leased.

The realization was immediate: the systems he depended on every day were part of the digital attack surface he thought didn’t exist. This lack of awareness is widespread, and dangerous.

Executive Summary

Smart buildings have become foundational elements of the 21st-century urban landscape. From commercial towers and government facilities to hospitals and university campuses, these structures are increasingly defined not by their architecture but by their intelligence. Specifically, their ability to optimize operations, reduce energy use, and deliver superior occupant experiences through connected technologies.

But this intelligence comes with a cost. The operational technology (OT) systems powering building automation, such as HVAC, lighting, elevators, fire safety, and access control—are now recognized as critical infrastructure. Yet many remain unprotected, invisible to security teams, and vulnerable to increasingly sophisticated cyber threats.

The Five Forces Driving the OT Cybersecurity Reckoning

A seismic shift is underway in cybersecurity and buildings are at its epicenter. The convergence of operational technology (OT) with IT networks, coupled with smart city ambitions and sustainability mandates, has transformed building systems into critical digital infrastructure. Five key forces are now reshaping how enterprises must think about OT and building cybersecurity:

1. THREAT SHIFT TO OT

Once peripheral, OT systems are now prime targets. Ransomware actors, cybercriminals, and nation-state groups are increasingly bypassing hardened IT environments to disrupt building controls, environmental systems, and access infrastructure.

2. REGULATORY PRESSURES ACCELERATE

Governments are catching up. Canada's Bill C-8 and similar regulations around the world are driving mandatory risk programs that include building systems. Compliance frameworks are no longer optional for owners of commercial, healthcare, financial, and public sector facilities.

3. CYBER INSURANCE IS WAKING UP

Insurance underwriters are beginning to see OT as uninsurable without visibility and controls. Renewals are now contingent on the inclusion of building system risks, and organizations are scrambling to catch up or risk denial of coverage.

4. CYBER WARFARE EXPANDS THE RISK HORIZON

Nation-state adversaries are increasingly leveraging OT systems as tools of disruption. Critical infrastructure, including smart buildings, is now viewed as a legitimate target for geopolitical leverage, hybrid warfare, or symbolic impact within smart cities.

5. THE SERVICES GAP IS DANGEROUS

The cybersecurity industry is not ready. There is a critical shortage of professionals, solution providers, and vendors capable of delivering OT-specific security services. When a widespread OT cyber event hits the real estate sector, demand will dramatically exceed supply.

1. Smart Buildings: The Backbone of Urban Innovation

Smart buildings are no longer niche innovations, they are becoming the standard. These structures use a blend of sensors, automation platforms, analytics, and remote connectivity to manage physical systems more efficiently. Building Automation Systems (BAS) and Building Management Systems (BMS) control critical functions including:

- Heating, ventilation, and air conditioning (HVAC)
- Lighting and shading systems
- Fire detection and suppression
- Elevator systems
- Physical access and surveillance

Protocols like BACnet/IP, Modbus, KNX, and LonWorks enable these systems to communicate. While they deliver substantial operational and environmental benefits, these protocols were designed for functionality—not security.

The global smart building market is projected to grow by 800% over the decade. The market is expanding at an average Compound Annual Growth Rate (CAGR) of approximately 24.4%. North America, Europe, and APAC are all seeing a surge in smart infrastructure as governments invest in smart city strategies and sustainable urban growth.

2. Cyber Risks Hiding in Plain Sight

OT systems in smart buildings often escape the attention of cybersecurity programs. Managed separately from IT, these environments are rarely subject to the same policies, controls, or monitoring.

KEY THREAT FACTORS:

- **Lack of network segmentation** between IT and OT systems
- **Use of default** or hardcoded credentials
- **Unsupported legacy** software in building controllers
- **Remote access tools** installed by vendors without proper vetting
- **Unencrypted** communication protocols vulnerable to interception or manipulation

INDUSTRY DATA HIGHLIGHTS:

- **Only 15% of** organizations globally have formal OT cybersecurity governance for buildings and 51% are insecurely connected to the internet, (Nozomi Networks)
- **Connected building** devices are widely targeted: ~33% of cyber attacks involve BAS-connected IoT devices—including connected elevators, HVAC systems, kiosks, and more. This highlights BAS as attractive threat vectors ([Fortinet](#))
- **Over 23,000 BAS** devices are currently discoverable via Shodan
- **OT assets account** for 42% of enterprise digital assets, but 64% of cyber risk exposure (Nozomi Networks)

These figures illustrate a gaping security blind spot at the heart of critical infrastructure. Beyond numbers, a compromised BAS can delay patient care, disrupt financial operations, or undermine public trust in critical institutions.

3. Real-World Breaches: Physical Impact, Digital Entry Points

Cyberattacks on building systems are no longer theoretical. They are happening today, with growing frequency and impact:

- **Las Vegas Casino** (2023): A fish tank thermostat was used as a pivot point into the main network.
- **Canadian Engineering Firm** (2022): A ransomware attack disrupted internal systems through an exposed BAS.
- **U.S. Hospital Campus** (2023): An HVAC vendor's remote access connection was used to disable access control systems.
- **Alberta Municipal Office** (2021): Ransomware locked down building automation terminals and fire interfaces.
- **Canadian University** (2020): Researchers demonstrated they could remotely override air handling setpoints.

These examples highlight how easily cyber threats can escalate into operational failures, especially in critical environments.

These breaches are not isolated events, they highlight why attackers increasingly see building systems as high-value opportunities.

4. Why Threat Actors Target Buildings

Buildings offer a high-value, low-effort target profile for cyber attackers:

- **Ease of entry** through unmonitored ports and outdated software
- **Operational disruption** leverage for ransom payments
- **Third-party access** points via vendors and integrators
- **Valuable data collection** on tenants, behavior, and physical systems
- **Symbolic impact** for geopolitical actors seeking visibility

These motivations make buildings a favored frontier for the next generation of cyber attacks.

With attackers focusing on buildings and regulators raising the stakes, the question is no longer if, but how, organizations can defend themselves.

So Where Do We Start?

"We can't defend what we don't know..."

The first step in building cyber resilience for smart buildings is visibility. But visibility must be paired with management, expertise, and continuous improvement. Protecting OT systems requires not just controls, but the ability to adapt them to the unique realities of the built environment.

A. DISCOVER, ASSESS & MANAGE

Knowing precisely which systems and assets are in place forms the foundation of defense. Organizations need to build a clear inventory of every controller, protocol, and vendor connection. From there, the goal is to create a plan that leverages technology to maximize visibility and response capabilities. This work cannot stop at identification—ongoing management is critical. A team of OT experts must be in place to mitigate daily risks, interpret anomalies, and continuously improve the defensive architecture as both threats and building systems evolve.

B. HARDEN & SEGMENT

Once visibility is established, the next step is containment. Network segmentation, VLANs, and protocol-aware firewalls prevent a single compromise from spreading across building systems. Hardening configurations and restricting remote access reduce the attack surface. However, this requires an understanding of how to apply changes without breaking core building functions.

C. MONITOR, DETECT & RESPOND (MDR)

Generic monitoring isn't enough, OT systems generate unique signals and operate on legacy protocols. Managed Detection and Response (MDR) for OT demands specialized expertise to keep these systems secure without disruption operations. OT-aware MDR services can spot abnormal activity in elevator controllers or HVAC systems long before IT tools would raise an alert.

D. RESPOND & RECOVER

The ability to withstand attacks depends on having defensible architectures that permit near real-time response. OT incident playbooks must consider not just digital assets but physical safety, ensuring that recovery plans bring buildings back online securely. The difference between hours of downtime and rapid recovery often comes down to having systems designed from the ground up for resilience. Building these defensible architectures enables organizations to withstand disruptions and maintain continuity, even during sustained attack.

E. GOVERN & VALIDATE

Governance ties everything together. OT security must be integrated into executive oversight, vendor contracts, and compliance reporting. Mapping compliance strategies to recognized industry standards (such as ISA/IEC 62443 or ISO 27001 for data security) ensures alignment with regulators and insurers, while embedding accountability across IT and facilities leadership. Embedding defensible architectures into governance frameworks ensures systematic resilience, not situational.

Governance policies must also be validated in practice. Regular workshops, tabletop exercises, and scenario-based drills confirm that policies are understood, responsibilities are clear, and controls work as intended. This transforms governance from static documentation into a living framework of accountability and resilience.

Conclusion: From Awareness to Defensible Architectures

Smart buildings are the digital skeleton of the modern city. They are no longer just energy systems—they are cyber-physical platforms critical to safety, sustainability, and business continuity.

Ignoring OT risk is no longer acceptable. The convergence of threat activity, regulation, insurance, and awareness demands a new posture: one of action, accountability, and

alignment. In this era of smart infrastructure, resilience begins not in the cloud, but in the building itself.

Components for the path forward are clear: visibility, hardening, OT-aware detection, real-time response, and strong governance. But these pillars are only effective when executed with the expertise of professionals who understand both engineering realities and cybersecurity imperatives.

Generic IT strategies cannot defend smart infrastructure on their own: defensible architectures that are designed and maintained by OT-specific experts enable organizations not only to withstand today's attacks but also to adapt to tomorrow's threats.

Enterprises that invest in this expertise will be best positioned to protect tenants, meet compliance obligations, satisfy insurers, and keep the buildings that power our cities running without interruption. In the digital skeleton of modern cities, defensible architectures are not optional—they are the line between safe, resilient infrastructure and critical failure.®

This article is vendor-neutral and reflects global research, real-world case studies, and regulatory insights current as of 2024–2025.

Tristan Kim is a cybersecurity visionary, entrepreneur, and growth strategist with over 17 years of experience building and advising security-first organizations across North America. As a Director of Cyber Risk, Innovation & Strategy at KORE Solutions, Tristan built and scaled the company's cybersecurity practice—positioning KORE as a specialist in securing smart buildings, BAS/BMS environments, and critical infrastructure through risk advisory, design, including a managed detection and response (MDR) capabilities for the OT world.

Under his leadership, KORE has become a trusted partner for building owners, facility operators, and real estate portfolios, while extending its OT cyber expertise to other high-risk sectors such as healthcare, transportation, and public infrastructure.


Youssef Jad is a CTO & Co-Founder @ CyVault™ (a division of PM SCADA Cyber Defense), leading Cyber Defense operations and novel R&D products. Has over 25 years of experience in IT/OT/ICS/CPS/xIoT cyber defense, consultant and advisor to Fortune 10 companies and leading industry organizations, and accomplishments include delivering turnkey cyber solutions for the US-Gov/DHS/FBI, contributing to offensive initiatives for cyber military units, and serving as a recognized subject matter expert (SME) for OT-focused organizations and laboratories including ISA (International Society of Automation) and INL (Idaho National Labs).



Pioneering MDR Specifically for Building Automation Systems



KORE

Powered by  cyvaalt™



Why Critical Infrastructure Must Prioritize Cybersecurity

by [Enza Alexander](#)

From power grids to hospitals, our modern world depends on operational technology (OT). But as these systems become more connected to traditional IT networks, they also become more exposed to today's relentless cyber threats. The stakes aren't just financial – they are human, societal, and existential.

This article explores the evolving threat landscape, sector-specific risks, emerging regulations, and the essential role of AI and resilience planning in securing Canada's national infrastructure.

The Evolving Threat Landscape Requires Proactive Risk Management

The convergence of OT and IT has significantly expanded the cyber attack surface on critical infrastructure (CI).

Legacy OT systems were not designed with cybersecurity in mind and are now exposed to modern threats. Ransomware-as-a-Service (RaaS), zero-day vulnerabilities, and AI-driven attacks are increasingly targeting CI. Cybersecurity in OT isn't just about networks or data. It also requires cyber professionals to understand that these systems were designed, and are often still supported, by professional engineers who prioritize public safety above all else.

Critical infrastructure sectors including energy, healthcare, water, and transportation, operate systems that, if compromised, can result in catastrophic consequences. Cyber attacks on industrial control systems (ICS) can disable safety mechanisms, causing explosions, chemical leaks, or power grid failures. Healthcare systems can be paralyzed by ransomware, delaying patient care and putting lives at

risk. Transportation systems, such as rail or aviation control networks, may be manipulated to cause large-scale accidents. These environments aren't just about data – they're about physical safety. A breach could directly endanger thousands of people.

A successful cyber attack on infrastructure can create ripple effects across global supply chains and national security frameworks, making resilience a geopolitical imperative.

“Public safety and human lives depend on OT system integrity.”

Canada's OT environments face pressure from all sides. Ransomware gangs exploit legacy systems, often targeting CI, where downtime can compromise outcomes and even cost lives. Nation-state actors are probing our critical infrastructure.¹ Hacktivists are looking for ways to make a statement. Insider risks, either in the form of malicious activity or unintentional actions² are of significant concern. Many OT systems were never designed for internet exposure: now that they are being connected to IT networks for efficiency, the attack surface has expanded dramatically. And we're seeing this play out in the real world: in 2024, 73% of reported cyber incidents affected OT systems in some way, up from just 49% the year before.³

The Canadian Centre for Cyber Security's (CCCS) [National Cyber Threat Assessment 2025-2026](#) confirms ransomware as the top cyber crime threat to our critical infrastructure. In energy, attackers understand the financial leverage of disrupting fuel or power distribution. In healthcare, attackers know they can force IT teams to make ransom payments due to the criticality of systems. These aren't opportunistic strikes - they're calculated moves.

Sector in Focus: Energy

Canadian energy providers face similar challenges. Legacy industrial control systems, complex supply chains, and remote operations all create vulnerabilities with potentially catastrophic results. A cyber attack that manipulates pressure sensors or disables safety alarms could lead to real-world disaster. In fact, I've personally spoken to some critical infrastructure executives who are opting to retain manual processes instead of automating, citing concerns with potential OT infrastructure attacks. That's how grave the risks are.

In April 2024, Reuters quoted a North American Electric Reliability Corporation (NERC) report that suggests power grids are becoming increasingly vulnerable, with the number of susceptible points in electrical networks growing

by about 60 per day. Weak points across grid software and hardware jumped to a range of 23,000 to 24,000 in 2024 — up from 21,000 to 22,000 the previous year.⁴

As reported by CCCS, foreign state actors are “almost certainly” probing our energy infrastructure and pre-positioning malware that could be used to disrupt or destroy systems in the event that a conflict breaks out. Meanwhile, ransomware groups are opportunistically targeting oil and gas companies, looking for a quick payout. The convergence of IT and OT means that a compromised office email can lead to control room access. Segmentation, monitoring, and response plans are no longer optional – they're essential.

Sector in Focus: Healthcare

In over two decades working with clients, I've seen dramatic change from an OT cybersecurity perspective. Twenty years ago, OT wasn't nearly as critical a component of our healthcare sector as it is today. These days, hospitals rely on complex networks of medical devices, HVAC systems, diagnostic platforms, and administrative tools – all forming an OT ecosystem that can be challenging to track, maintain, and protect. Securing these devices is difficult; patches may be hard to apply, if available at all. There's zero tolerance for downtime. Meanwhile, clinical staff face overwhelming demands, and cybersecurity often competes with immediate care priorities.

And the risks are real. Consider the 2024 Ascension ransomware incident⁵ in the United States. A ransomware attack by the Black Basta gang forced Ascension to shut down its OT networks and electronic health record systems across 142 facilities, severely disrupting healthcare services. Surgeries and appointments were delayed, ambulances diverted, and pharmacies and labs reverted to manual processes as digital systems went offline. Many hospitals operated on paper records for weeks, leading to slowdowns and patient safety concerns. The breach, which stemmed from an employee accidentally downloading a malicious file, ultimately affected 5.6 million individuals.

“Whether in power plants or hospitals, cyber threats don't wait for modernization. They exploit what's already online.”

Compliance and Regulatory Response

Critical infrastructure forms the backbone of a nation's economy and security. Sophisticated cyber attacks, especially those from nation-state actors, target CI to: disrupt

essential services (e.g., fuel pipelines, water treatment, telecommunications); cause financial loss through downtime, recovery, and regulatory penalties; and undermine public confidence in government and private institutions.

In 2022, Canada's Bill-26 was introduced, with a goal of strengthening Canada's national cybersecurity framework by giving the federal government broad powers to protect critical infrastructure. Though Bill C-26 was shelved following the January 2025 prorogation of Parliament, its replacement, Bill C-8,⁶ was introduced in June 2025 as a renewed legislative effort to bolster national cybersecurity. It comprises two main components: amendments to the Telecommunications Act and the introduction of the Critical Cyber Systems Protection Act (CCSPA). These measures aim to empower federal authorities to direct telecommunications providers in safeguarding Canada's infrastructure against cyber threats, including potential interference and manipulation. Non-compliance could lead to significant penalties or imprisonment, underscoring the government's commitment to modernizing its approach to cybersecurity and protecting critical national systems.

Alongside this proposed legislation is the Canadian Program for Cyber Security Certification (CPCSC), a new standard for national defense contractors and supply chain partners. Launched in 2025, CPCSC is Canada's equivalent of the U.S. CMMC, requiring cybersecurity certification before a firm can bid on sensitive government projects. While it starts in defense, there is potential for this model to be extended across other sectors. It sets a baseline, creates competitive advantage for certified firms, and raises the bar for national cyber hygiene.

Meanwhile, evolving standards and frameworks like [NERC CIP](#) (for power system cybersecurity), [NIST CSF](#) (a U.S. risk management framework), [IEC 62443](#) (industrial automation security), and more, are highlighting the importance of compliance and best practices. Without modern safeguards, CI operators risk falling behind attackers.

"National security and economic stability are at stake."

The AI Factor

And of course, there's the AI factor. Canada's appointment of its first-ever Minister of Artificial Intelligence and Digital Innovation in May 2025 underscores the nation's commitment to this revolutionary technology. Secure AI development and governance is a strategic national priority.

Andrew Buckles, EVP of Cyber Services at ISA Cybersecurity, and a thought leader in the field of artificial intelligence, recognizes the impact of AI in the OT environment. He offered this example: "Think about monitoring security cameras. Even if they are analog, AI could recognize someone approaching the door and unlock it without a badge or retinal scan."

He observes that, "for native IoT devices, AI will play a huge role in supporting these types of systems, (and while) regulation(s) and legislation may slow the pace of AI adoption in this space; at this stage, that's probably a good thing."

My friend and colleague, John Jaisaree, is a professional engineer and a pioneer in integrating artificial intelligence into automation and OT. We've had many conversations about public safety and the national security implications of securing OT, ICS and IIoT systems. As John recently wrote, "In 2024, state-sponsored hackers utilized AI tools, such as ChatGPT, to map and exploit water treatment

plants. This isn't sci-fi. It's happening now—and the front line is ICS and OT systems.”

“The potential of AI is powerful—and so is the risk.”

A Call to Action

Get informed and use the resources that are out there. Talk to partners and industry groups to share knowledge and best practices. The Cybersecurity Infrastructure Security Agency (CISA) consistently adds new vulnerabilities to its [Known Exploited Vulnerabilities \(KEV\) Catalog](#), informed by evidence of active OT exploitation.

I recently participated in a tabletop exercise simulating an attack on municipal CI, including its OT networks. If you've never participated in one, they are real eye-openers. These cyber drills illustrate the importance of teamwork and communication in effectively managing a cyber incident that could affect thousands of people. The threats we face are complex and fast-moving; no one can tackle them alone.

I've often said that cybersecurity isn't just a job—it's a calling. Cybersecurity is no longer the sole responsibility of IT professionals. Boards, regulators, engineers, and frontline operators all have a role to play. From the factory floor to the emergency room, we must build cultures of security. We must put a priority on incident response, modernization, intelligence sharing, and bridging IT-OT gaps to protect lives and critical infrastructure. This means protecting OT and CI systems as carefully as we deploy them. It's imperative that we share intelligence – because the bad actors do.

“Resilience starts with readiness. Cybersecurity shouldn't be bolted on—it needs to be baked in.”®

See [end notes](#) for this article's references.

Enza Alexander is Executive Vice-President at ISA Cybersecurity, one of Canada's leading cybersecurity services and solutions providers. Enza is a seasoned IT industry leader with over 30 years of experience across the technology sector. She is passionate about helping clients understand how strong information security management systems can keep them cyber safe. Her extensive experience in the energy, utility, and health-care sectors forms the foundation of her operational technology (OT) expertise.

In 2022, Enza was named one of Canada's Top Women in Cybersecurity by IT World Canada (ITWC) and a trailblazer woman leader by *Aspioneer Magazine*. In 2011, Enza was recognized as one of Canada's leading Women in Technology by IT Canada and *CDN Magazine*.



From Guidelines to Guardrails: The Power of Deploying Cybersecurity Standards in Canada's Industrial Sector

by [Denrich Sananda](#) and [Sonia Khan](#), Presented by Arista Cyber

Executive Summary

As Canada's industrial and critical infrastructure sectors embrace digital transformation, the need for robust cybersecurity in operational technology (OT) and industrial control systems (ICS) has never been more pressing. Cyberattacks on energy, transportation, and manufacturing sectors are increasing in frequency and sophistication. This article outlines the importance of adopting recognized cybersecurity standards and frameworks within the Canadian industrial sector. By doing so, organizations not only improve their resilience and compliance but also align with evolving regulatory landscapes.

Introduction

Industrial systems in Canada have undergone a dramatic shift from once-isolated, air-gapped environments to interconnected ecosystems that rely heavily on digital communication, real-time analytics, and remote access. While this evolution has enabled efficiency and innovation, it has also exposed OT systems to a growing spectrum of cyber threats.

From ransomware attacks targeting pipelines to the compromise of ICS, recent events have underscored the need for sector-specific cybersecurity practices.

The challenge is not just about technology. It's about readiness, responsibility, and resilience. And at the heart of this preparedness lies a clear understanding and application of cybersecurity standards and frameworks—tools that are no longer optional, but vital for national safety and industrial integrity.

Understanding the Cybersecurity Building Blocks: Standard vs. Framework vs. Governance vs. Compliance

To build a resilient cybersecurity program, it's important to understand foundational concepts:

Standard: A documented set of rules or requirements developed by recognized bodies (e.g., ISO, IEC) to ensure consistency and best practices in specific processes.

Framework: A broader strategic approach that offers guidance on how to manage cybersecurity risk. It provides structure but may not mandate specific controls.

Governance: The system by which organizations are directed and controlled in relation to cybersecurity, including policies, responsibilities, and oversight.

Compliance: The act of meeting the requirements outlined in applicable laws, regulations, and standards.

Regulation: A legal obligation enacted by a government or regulatory body that mandates specific actions, reporting, or controls. Non-compliance can result in penalties.

In OT cybersecurity, these elements work together; frameworks guide strategy, standards define control expectations, governance ensures accountability, and compliance confirms alignment with requirements.

Cybersecurity Standards and Frameworks in Focus

CSA Z246.1:21 – CYBERSECURITY FOR INDUSTRIAL AND CRITICAL INFRASTRUCTURE

- **Overview:** A Canada-specific standard developed by the Canadian Standards Association (CSA), tailored for the unique needs of IACS environments. It aims at safeguarding and enhancing the resilience of Canada's oil and gas, petrochemical and mining infrastructures.
- **Relevance:** Provides guidance on cybersecurity risk management across the lifecycle of IACS; from design and installation to maintenance.
- **Current Adoption:** Recommended across oil & gas, utilities, and manufacturing sectors. Frequently cited in provincial regulations.

- **Unique Value:** Tailored to Canadian regulatory context and harmonized with international standards such as IEC 62443.

ALBERTA REGULATION 84/2024 – SECURITY MANAGEMENT FOR CRITICAL INFRASTRUCTURE REGULATION

- **Overview:** This regulation is part of the Responsible Energy Development Act and aimed at creating comprehensive security management protocols for critical infrastructure in Alberta's energy sector.
- **Relevance:** Applies to sectors such as energy, utilities, and transportation, requiring them to implement cybersecurity programs aligned with recognized standards.
- **Current Adoption:** Legally enforced in Alberta as of 2024. Effective May 31, 2025, Alberta Regulation 84/2024 will mandate compliance for defined critical facilities.
- **Unique Value:** First provincial regulation of its kind in Canada to require cybersecurity baselines in OT environments.

BILL C-8 (FORMERLY C-26) – CRITICAL CYBER SYSTEMS PROTECTION ACT (CCSPA)

- **Overview:** Canadian federal legislation aimed at improving cyber resilience in vital infrastructure sectors such as finance, energy, and transportation.
- **Relevance:** Establishes mandatory reporting, risk mitigation, and incident response requirements for designated operators.
- **Current Status:** Introduced in Parliament and renamed from Bill C-26 to Bill C-8. Still undergoing legislative process.
- **Unique Value:** Moves cybersecurity from a voluntary practice to a mandated requirement for critical sectors. Emphasizes regulatory oversight.

NIST CYBERSECURITY FRAMEWORK 2.0

- **Overview:** A globally recognized framework from the U.S. National Institute of Standards and Technology.
- **Relevance:** Widely used in Canada, especially in energy and utilities sectors, for aligning risk management practices.
- **Structure:** Based on five core functions: Identify, Protect, Detect, Respond, and Recover.
- **Unique Value:** Flexible and scalable, compatible with ISO/IEC 27001 and IEC 62443.

IEC/ISA 62443 – THE INDUSTRIAL CYBERSECURITY BACKBONE

- **Overview:** An international series of standards developed by ISA and adopted by IEC for securing IACS environments.
- **Relevance:** Considered the gold standard for OT cybersecurity. Covers asset owners, system integrators, and product suppliers.
- **Current Adoption:** Increasingly integrated into procurement and lifecycle management practices.
- **Unique Value:** Lifecycle-focused. Promotes defense-in-depth, zones and conduits, and security level requirements.
- **Risk-Based Approach:** IEC 62443 encourages a risk-based methodology by classifying assets, identifying potential threats, and assigning Security Levels (SLs) based on the consequence of compromise. Organizations perform a cybersecurity risk assessment to determine appropriate SLs for zones and conduits, ensuring that mitigations are proportionate to risk. This approach enables targeted investments, improves control granularity. It also ensures that security controls are aligned with operational needs and threat exposure, a critical consideration in environments where availability and safety are paramount.

IEC/ISO 27001 – INFORMATION SECURITY MANAGEMENT

- **Overview:** A well-known standard for establishing and maintaining an information security management system.
- **Relevance:** While originally IT-focused, it provides a useful governance and risk management model for OT environments.
- **Current Adoption:** Often forms the backbone of enterprise cybersecurity strategies in Canada.
- **Unique Value:** Complements technical OT standards with strong policy and procedural controls.

Standards Aren't Just Paper: Real Benefits

In today's threat-laden digital environment, cybersecurity standards are far more than technical documentation, they are strategic safeguards, purpose-built to protect Canada's most vital operations. The increasing convergence of IT and OT systems has dramatically widened the attack surface across critical infrastructure sectors such as energy, water, manufacturing, and transportation. These sectors are no

longer shielded by airgaps or physical isolation. They are digitally connected, exposed, and in many cases, unprepared.

Real world incidents such as the Colonial Pipeline ransomware attack and the Triton malware that targeted safety instrumented systems have made it painfully clear: cyberattacks on OT environments don't just steal data, they can halt fuel delivery, shut down power grids, endanger worker safety, and negatively impact the national economy. These events underline the need for structured, proactive approaches to cybersecurity, and this is precisely where standards and frameworks come into play.

Organizations that align with these standards position themselves not just for regulatory success, but for stakeholder confidence, customer assurance, and operational continuity.

Rather than relying on fragmented defenses or reactive protocols, recognized standards and frameworks such as CSA Z246.1:21, NIST CSF 2.0, and IEC 62443 offer an organized and validated path toward cyber resilience. They embed security into the DNA of industrial operations—defining best practices for access control, system hardening, network segmentation, monitoring, and incident response.

Compliance with these standards is also fast becoming a regulatory imperative. Bill C-26 (now Bill C-8) signals a clear shift from voluntary best practices to mandated cybersecurity governance across Canada's critical infrastructure sectors. Organizations that align with these standards position themselves not just for regulatory success, but for stakeholder confidence, customer assurance, and operational continuity.

Adopting standards is an investment in maturity. It means moving from a reactive to a proactive security posture, one where risks are continuously assessed, gaps are identified before exploitation, and teams are prepared to respond with speed and precision. Standards also support the

creation of playbooks, escalation protocols, and training programs that prepare not just the IT team, but the entire workforce to act decisively in the face of a cyber event.

Ultimately, these frameworks act as a unifying language across departments, technologies, and industries. In a time when cyber risk is a boardroom conversation and a plant-floor reality, cybersecurity standards offer the clarity and consistency needed to protect Canada's industrial future.

Looking Ahead: The Future of OT Cybersecurity in Canada

Canada is at a pivotal point. As digital transformation accelerates, industrial operators must treat cybersecurity as a critical enabler and not just a cost. The convergence of operational and informational technologies brings both efficiency and risk.

We anticipate broader enforcement of cybersecurity legislation, increased demand for certified frameworks, and deeper integration of AI and machine learning in threat detection. Additionally, workforce training and sector-specific implementation guidance will be key to making these standards effective at ground level.

Conclusion

Canada's OT/ICS sector is a cornerstone of national stability and economic vitality. As cyber threats evolve, so must our defenses. Standards and frameworks like CSA Z246.1:21, Bill C-8, NIST CSF 2.0, IEC 62443, and ISO 27001 are not just checklists, they are blueprints for survival in a connected industrial world. By adopting and embedding these frameworks, Canadian industries can comply with emerging regulations while also building safer, more resilient operations capable of withstanding the next wave of cyber threats. ⁸

See [end notes](#) for this article's references.

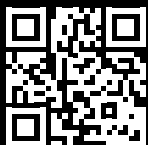
[Denrich Sananda](#) is Managing Partner at Arista Cyber and a seasoned Industrial Cybersecurity Consultant with extensive experience in securing Operational Technology (OT) environments. With a background in automation and a deep understanding of standards like NERC CIP, ISA/IEC 62443 etc., he specializes in assessing and mitigating cyber risks in critical infrastructure sectors across Canada and Middle East. Denrich has worked on high-profile projects in energy, utilities, and transit systems, helping organizations enhance their resilience against evolving cyber threats.

[Sonia Khan](#) is a Cybersecurity Consultant at Arista Cyber, specializing in securing Industrial Control Systems (ICS) and Operational Technology (OT) environments. With a Master's degree in Electrical and Software Engineering (UCalgary) and a background in research and teaching, she brings both technical expertise and practical insight to safeguarding Canada's critical infrastructure. Her work focuses on developing secure, innovative solutions to strengthen the resilience of critical ICS environments.



WHEN OT STOPS, THE WORLD STOPS. **ARISTA CYBER** **KEEPS IT RUNNING** **SECURELY**

We unite human-centric strategy with world-class expertise to deliver cybersecurity that is simple, safe, and effective.



More information: aristacyber.io
Contact us: info@aristacyber.io

The Cutting Edge
of OT
Cybersecurity



Defence vs. Commercial: Not So Different When Protecting Critical Assets

By Daly Brown and Nick Foubert

If you look up any definition of critical infrastructure it always refers to some combination of the assets, systems, and networks that are essential to a functioning society. This can include things like energy grids, transportation systems, water treatment facilities, and financial institutions.

Dig a bit deeper and you'll find these systems are built on a foundation of operational technology (OT) — the hardware and software used to monitor and control physical

processes, devices, and infrastructure. These OT systems are integral to critical infrastructure, managing everything from the flow of electricity in energy grids, to the precise movements of machinery in manufacturing systems, to the purification processes in water treatment facilities.

Now consider defence infrastructure and, more specifically, the assets essential to military operations. These include weapon systems, military communication networks,

command and control systems, surveillance platforms, and other supporting defence capabilities.

Same Same But Different

Defence and critical infrastructure assets, despite their seemingly disparate domains, share a striking resemblance in their operational reliance on networked systems of sensors, actuators, and effectors. This interconnectedness forms the backbone of both military capabilities and essential civilian services. In essence, a networked battlefield, constantly gathering intelligence through sensors, executing commands via actuators, and carrying out actions through effectors, is not so different from a connected industrial control system managing, for example, a power grid or a water treatment facility.

Similarly, they both represent high-value targets for adversaries for their strategic importance. When compromised, the impacts could lead to catastrophic outcomes that range from widespread societal disruption and economic collapse to loss of life and significant national security implications.

Moreover, both defence and critical infrastructure systems often operate in isolated or highly controlled environments, with longer lifecycles for specialized hardware and software. Upgrades and patches can be challenging due to the need for extensive testing, re-certification, and their continuous operational usage.

However, the security models of defence and critical infrastructure have prioritized the classic triad of confidentiality, integrity, and availability (CIA) differently. In defence, confidentiality and integrity were often paramount for intelligence, surveillance, and reconnaissance systems. The unauthorized disclosure of military intelligence could have immediate and catastrophic national security implications. For critical infrastructure, availability and integrity were typically the highest priorities. The disruption of an energy grid, water treatment facility, or transportation system directly impacts public safety and economic stability.

In recent years, the lines between these priorities have begun to blur. The increasing interconnectedness of systems, real-time information sharing, remote operations, and protected industrial processes has necessitated a more balanced approach to the CIA triad in both sectors, one that preserves strategic advantage and reinforces operational resilience. The proliferation of artificial intelligence (AI) and the anticipated arrival of quantum computers has only underscored this, presenting new cybersecurity challenges that demand advanced and integrated security solutions.

Emergence Of Dual-Use Technologies

The defence and critical infrastructure sectors are increasingly recognizing the value of shared security principles and solutions. Digital transformation in both sectors is accelerating as operators recognize the benefits of increased connectivity and digitalization. However, this transition also inherently expands their attack surfaces, and in both scenarios, the consequences of subversion are severe, highlighting the importance of robust security measures and the potential for dual-use technologies.

The evolving landscape of cyber threats has led to a significant convergence in cybersecurity approaches for both defence and critical infrastructure sectors. Regulatory and advisory bodies are increasingly recognizing this overlap. This has led to the development of new and updated regulations and standards, and many of which apply to both domains. As a result, both sectors are adopting state-of-the-art methods, techniques, technologies, and processes for cybersecurity.

Join The Buzzword Parade

In the April 2023 report [Shifting the Balance of Cybersecurity Risk](#), the U.S. Cybersecurity and Infrastructure Security Agency (CISA) asserts that technology manufacturers must prioritize secure-by-design and secure-by-default in product design and development.

In February 2024, the White House released [Back to the Building Blocks: A Path Toward Secure and Measurable Software](#), calling on critical system designers to shift their perspective on cyber vulnerability from reactive to proactive. It urges for the proactive elimination of entire categories

of software vulnerabilities through advanced engineering techniques, before deployment. This philosophy will set a new benchmark for secure technologies in both sectors.

The following techniques are just some of the ways in which organizations are building technology to meet this new standard. And this isn't hype—these are proven techniques recommended by some of the most technically sophisticated and knowledgeable organizations out there.

Formal methods

The increasing availability of computing resources has enabled the practical application of formal methods in real-world software development, allowing for automated program analysis and verification of complex systems that was previously infeasible. State-of-the-art formal methods and verification tools are now being integrated into modern software development processes, enabling developers to detect and eliminate entire classes of vulnerabilities early in the development lifecycle. These techniques are further explored in the January 2025 CISA report [Closing the Software Understanding Gap](#).

Memory safety

Industry leaders and government agencies, including the Canadian Centre for Cyber Security (CCCS), CISA, and the National Security Agency (NSA), are advocating for the adoption of memory-safe programming languages due to their proven ability to enhance software security, as outlined in their December 2023 joint report [The Case for Memory Safe Roadmaps](#).

Zero trust

Zero trust represents a fundamental shift away from traditional network perimeter-based security by embracing the principle of “never trust, always verify” for all users, devices, and applications, regardless of location. This aligns with the modern understanding that threats can originate from anywhere given increasingly complex and distributed IT and OT environments. The 2023 report from the CCCS [A zero trust approach to security architecture](#), highlights how zero trust is widely considered the current best practice for security architecture.

Data-centric security

This technique shifts the focus from securing perimeters to protecting data itself. It does so through encryption and access controls based on identity, context, and least privilege. It also incorporates data classification and discovery that identifies sensitive data and applies appropriate protection. Security metadata is embedded within the data, allowing protection mechanisms like encryption and access controls to travel with it. These safeguards remain effective even when the infrastructure is compromised or untrusted, such as in cloud environments or when data is shared externally. This approach aligns with the zero trust principle of “don't trust any network, including your own” and serves as a guiding principle of the Department of National Defence and Canadian Armed Forces 2024 [Artificial Intelligence Strategy](#).

Crypto agility

Quantum computers could render current encryption methods obsolete, creating a future where encrypted data stolen today may be decrypted once quantum capabilities mature. There is a need to future-proof systems against emerging quantum threats and vulnerabilities within cryptography platforms. The concept of crypto agility and the ability to rapidly adapt cryptographic methods in response to evolving threats, is gaining prominence. Its importance is emphasized in the October 2024 report from CISA [Post-Quantum Considerations for Operational Technology](#), which encourages vendors and operators to prepare for this inevitability.

Conclusion

The similarities between protecting defence and critical infrastructure assets cannot be understated, particularly in their shared reliance on networked operational technologies. They are both exposed to a rapidly evolving threat landscape and remain vulnerable as high-value targets. Increasing interconnectedness and new threats like AI and quantum computing are necessitating a converged, proactive approach to cybersecurity. It is no longer sufficient to just respond to attacks, industry must collaborate, particularly between commercial and defence sectors, to leverage shared expertise and innovation in cybersecurity to proactively address evolving global threats.

Canada has long established itself as a pioneer and innovator in artificial intelligence, cyber resilience, defence systems integration, and quantum technologies. With the federal government's recent focus on expanding core military capabilities, reindustrialization, and infrastructure building, there is a generational opportunity for innovators in both sectors to build the technologies of tomorrow: safe, secure, and reliable, by design and default.®

Daly Brown is Co-Founder and CEO and Nick Foubert is Co-Founder and CTO of Metropolitan Technologies. Combined they have over 30 years of experience in aerospace and defence responsible for the design, development, testing, and deployment of mission-critical applications to air, land, sea, and cyber platforms. Their latest venture is focused on connectivity and cybersecurity of critical infrastructure assets for both defence and commercial applications.





How to Establish a CCSPA-Compliant Cybersecurity Program for Critical Cyber Systems

by [Sandeep Lota](#), Presented by Nozomi Networks

After a long and winding legislative journey, Canada is poised to pass its first major cybersecurity bill designed to protect both telecommunications and critical infrastructure. If passed later this year, the second part of Bill C-8 will enact the Critical Cyber Systems Protection Act (CCSPA) which, among other things, requires designated operators in key industries to establish a cybersecurity program for their critical cyber systems. As consequential as the CCSPA is, the impetus for Bill C-8 (and its predecessor, Bill C-26) lies in the first part, which amends the Telecommunications Act to allow the government to prohibit the use of products or services that pose a threat to

Canada's telecommunications system. This article will focus on helping designated operators in key industries meet the CCSPA requirements.

Background: From C-26 to C-8

On June 18, 2025, the Canadian Minister of Public Safety introduced into Parliament Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. The bill resurrects Bill C-26, which passed the Senate in December 2024 but died on the order paper when Parliament

was prorogued in January 2025 after a drafting error. Reintroduced six months later as Bill C-8, the new bill is nearly identical to the original version, except for a few updates to procedural requirements. As such, it is expected to pass quickly.

Overview of the CCSPA

The CCSPA establishes a framework to protect cyber systems that support services vital to Canada's national security and public safety, imposing cybersecurity obligations on key sectors such as:

- **Telecommunications services**
- **Interprovincial or international pipeline and power line systems**
- **Nuclear energy systems**
- **Transportation systems** within the legislative authority of Parliament
- **Banking systems**
- **Clearing and settlement systems**

Designated operators in these industries must:

- **Establish a cybersecurity program** for their critical cyber systems
- **Mitigate supply-chain and third-party risks**
- **Report cybersecurity incidents** above a certain threshold
- **Comply with cybersecurity orders**
- **Follow information disclosure** and confidentiality rules
- **Keep records of their cybersecurity program** and any cybersecurity incidents

Penalties for non-compliance are up to \$1 million for individuals or \$15 million in any other case.

Getting Started: NIST CSF 2.0 and IEC 62443

The core obligation in the CCSPA is establishing a cybersecurity program for critical cyber systems. If you're starting from scratch and are unfamiliar with how securing operational technology (OT) and Internet of Things (IoT) devices differs from traditional IT tools and methods, this may be a heavy lift. Two leading cybersecurity frameworks provide trusted guidance: the [NIST Cybersecurity Framework \(CSF\) 2.0](#) and [IEC 62443](#), which are often used in conjunction.

Many CISOs are already familiar with NIST CSF, which was originally designed to help critical infrastructure organizations manage IT cyber risk. Developed by the National Institute of Standards and Technology in the U.S. and adopted globally, it offers a broad, flexible approach that is easy to implement and provides a clear path to maturity. The original framework outlines five core functions: Identify, Protect, Detect, Respond and Recover. Updated in 2024, version 2.0 added a sixth core function, Govern, with significant emphasis on OT, IoT and supply chain risk.

Developed by the International Society of Automation, IEC 62443 is a widely recognized standard for industrial cybersecurity. Part 2-1-2009 provides detailed guidance on establishing a high-quality industrial automation and control systems (IACS) security program.

The Four Steps to Establishing a Compliant Cybersecurity Program

The CCSPA outlines four steps designated operators must include in their cybersecurity program:

- **Identify and manage** any organizational cybersecurity risks, including those associated with supply chain and third-parties
- **Protect its critical cyber systems** from being compromised
- **Detect any cybersecurity incidents** that affect or could affect these systems
- **Minimize the impact** of cybersecurity incidents

The CCSPA also includes a fifth requirement: to comply with any additional measures prescribed by future regulation, a catchall that remains undefined until those regulations are published. The other four requirements form the foundation of any cybersecurity program, though formal approaches to managing supply chain and third-party risks have only matured in recent years.

Let's consider each step separately.

1. IDENTIFY AND MANAGE CYBERSECURITY RISKS

Before you can manage risk, you need to know what's connected to your network and what it's talking to. For designated operators, that means maintaining an automated inventory of all IT, IoT and OT assets, continuously updated with details on asset behavior and known vulnerabilities. In complex environments where unplanned downtime isn't tolerated, creating a complete asset inventory will likely require a variety of sensors and discovery methods to build

detailed asset profiles, ideally enriched using artificial intelligence (AI).

These capabilities will give you the asset and network visibility needed to identify and manage risk in your environment:

- **A variety of sensor types**, including network, endpoint and wireless, to monitor your entire environment
- **Active and passive discovery** techniques, with remote collectors to cover hard-to-reach and unmanned locations
- **Deep packet inspection (DPI)** and comprehensive OT, IoT and IT protocol fluency to analyze network traffic and understand behavior
- **An AI engine that learns** from millions of monitored assets to fill gaps about identical devices across environments and improve inventory accuracy.

Enlisting AI to enrich device profiles may sound like a nice-to-have, but it's a potent one. According to the SANS 2024 State of ICS/OT Cybersecurity, AI adoption among defenders is still nascent, with only 10% of respondents using AI in both enterprise IT and OT networks. That percentage is likely to surge as security teams begin to realize they must keep up with their adversaries, who are using AI to increase the sophistication and velocity of their operations.

Assessing and Prioritizing Risk

A complete asset inventory makes it easy to identify risk; the harder part is assessing its potential impact and knowing what to prioritize. Unlike IT cybersecurity, OT asset risk entails more than vulnerabilities. Patches (assuming they exist) must often be delayed until the next maintenance window. You must consider both cyber and operational risk down to the process variable level. When a pressure value spikes, you don't know if it is due to malicious tampering or operator error until the incident has been investigated. In an OT network, every component is part of a larger process, so risk is interconnected. Most importantly, the stakes are higher, failures can endanger people and harm the environment.

When looking at your OT asset risk, it's essential to identify which assets pose the greatest risk, whether by zone, site, vendor, or any other relevant category. You should be able to drill down to understand what makes them risky and what you can do about it. That's where automated risk scoring comes in. For OT devices, risk scores must account for more than just vulnerability risk but also:

- **Alert risk:** Measures how frequently the asset triggers security alerts. Higher volumes of confirmed or correlated alerts indicate increased exposure or likelihood of compromise.
- **Communication risk:** Evaluates what an asset communicates with and how. If the asset connects to untrusted or internet-facing systems, traverses network boundaries, or engages in unexpected or unauthorized traffic patterns, it's risky. DPI and protocol behavior analysis can uncover such risk.
- **Device risk:** Considers the device's inherent characteristics, such as its role (PLC, HMI, etc.), OS type, patch levels and known vulnerabilities. An unpatched legacy device running outdated firmware is risky.
- **Asset criticality:** Reflects how important the asset is to operational continuity and safety. This is typically defined by the organization (crown jewel assets, for example) and takes into account the asset's function within an industrial control system.
- **Compensating controls:** Policies and protections (network segmentation, endpoint monitoring, access control, etc.) in place that reduce the asset's effective risk. These controls may limit exposure, shorten response times or both.

Many cybersecurity platforms calculate multifactor risk scores, but if you're going to rely on them, you want to be able to customize the weight of each factor to reflect how your organization assigns risk. Risk scores help cut through the noise so your security team can zero in on the assets that matter the most. The right platform doesn't just calculate scores, it prioritizes them and gives clear guidance on which fixes will reduce the most risk.

Managing Supply Chain and Third-Party Risk

The CCSPA specifically obliges designated operators to manage supply chain and third-party risk, but doing so remains a challenge. A comprehensive asset inventory should include not only the asset itself but also its OS, end-of-sale and end-of-support dates, firmware version, and all software components, including open-source. Software bills of material (SBOMs) are the definitive source of information for managing supply chain and third-party product risk. As they become mandatory and more widespread, scanning SBOMs to pinpoint assets with vulnerable components will become easier. Leveraging AI to enrich asset profiles with complete information helps identify assets with high-risk components and determine whether to remediate or isolate them, making it the most effective course of action.

2. PROTECT CRITICAL CYBER SYSTEMS FROM BEING COMPROMISED

Network segmentation is fundamental to protecting critical cyber systems. With full network visibility, a well-defined segmentation architecture can efficiently break down large, flat networks into secure, manageable zones organized by function, criticality or geography, making policy enforcement much easier. If a threat actor gains access to one segment, they're prevented from pivoting to other sensitive areas, for example, from an HVAC system to a PLC that controls turbine operations.

Converged networks are the norm today, and critical infrastructure is no exception. Separating IT, IoT and OT networks should be the norm. Yet, recent surveys show that 50% to 75% of cyberattacks targeting OT systems originated in IT networks. Too often, unwanted communication links go unchecked under the assumption that these networks are separated when they are not. Attackers know this.

Yes, converged machines, devices and controllers must talk to each other to make operations more efficient, but those communications must be tightly controlled. The Purdue Model facilitates proper segmentation in industrial environments.

Although not originally designed as a cybersecurity framework, the Purdue Model has become the de facto reference architecture for segmenting process control networks. Widely adopted by OT engineers, it logically separates functions across five levels, with physical functions (equipment) at Level 0 and business functions (IT) at Level 4. To reduce risk, direct communication between Levels 3 and 4, such as a SCADA historian sending data to an enterprise resource planning system, is blocked by firewalls. Instead, all data exchanges must pass through a demilitarized zone (DMZ) at Level 3.5.

Beyond segmentation, isolation is often appropriate for assets including:

- **Certain legacy controllers** that make easy targets for adversaries
- **Safety critical systems** that, if compromised, could cause human or environmental damage
- **Crown jewel assets** such as primary SCADA servers, historian databases and central DCS controllers that could result in a full process compromise if breached

3. DETECT ANY CYBERSECURITY INCIDENTS THAT MAY AFFECT CRITICAL CYBER SYSTEMS

Detecting cyber incidents requires continuous monitoring, performed by the same sensors used to maintain an accurate asset inventory. As mentioned earlier, you must be able to detect both cybersecurity threats and operational anomalies, because until investigated, you don't know which it is. Comprehensive risk monitoring combines rule-based threat detection with behavior-based anomaly detection.

Rule-based Threat Detection

Rule-based detection is efficient for detecting threats where the indicators are easily observable and identifiable. This method can also be used to detect known, non-malicious anomalies, such as spikes in resource usage or an unexpected surge in traffic.

Signature-based detection (a subset of rule-based detection) is a fast, efficient way to detect malicious activity or unauthorized access. It works by using predefined rules to identify known attack patterns and matching them against a database of threats. An OT/IoT-focused threat intelligence feed helps ensure your sensors can detect the latest vulnerability signatures as well as emerging malware and indicators of compromise (IOCs).

Behavior-based Anomaly Detection

Operational anomalies and unknown threats, including zero-day attacks, can't be detected using rules. The best way to detect these threats is through continuous monitoring. DPI parses industrial protocols and compares current behavior against a baseline. AI and machine learning help establish these baselines and alert on deviations. To reduce nuisance alerts, thresholds must be set to filter out benign anomalous activity.

4. MINIMIZE THE IMPACT OF CYBERSECURITY INCIDENTS AFFECTING CRITICAL CYBER SYSTEMS

With a complete and accurate asset inventory, thoughtful network segmentation, and robust threat and anomaly detection, you will be well positioned to minimize the impact of cybersecurity incidents in your environment, including multi-stage attacks. More is more: the greater the variety of sensors you deploy (network, endpoint, wireless), and the broader the monitoring techniques and intelligence sources you use (passive DPI, selective active querying), the more quickly you can detect suspicious events and cut response time.

Even so, response actions should be deliberate and risk-calculated. Don't expect to cut and paste incident response plans from IT templates. In OT environments, safety and

process continuity take priority. That's why responses must be tightly coordinated with engineering and safety teams, who often are the better source for response tactics involving containment or shutdown steps.

An AI-powered cloud platform can significantly reduce workload by consolidating data from network traffic,

wireless signals, endpoint activity, behavior baselines and threat intelligence. This centralization streamlines risk management across sites and regions. One of AI's greatest strengths for defenders is automation, sorting and correlating data, prioritizing critical threats, adding context, and recommending next steps.

Level Up Your Critical Cyber System Security to Manage Enterprise Risk

The CCSPA is enabling legislation. As such, it establishes a broad framework, with details to be filled in by regulations after its passage. Ahead of those specifics, designated operators should be rolling up their sleeves and getting to work.

For CISOs, this means incorporating often-overlooked industrial control systems in your enterprise risk strategy. As CISOs increasingly assume responsibility for OT and IoT security, even those with mature IT cybersecurity programs are realizing a gap: they no longer have the cyber maturity they thought they did without developing a cybersecurity program tailored to these assets.

The OT/IoT cyber maturity curve begins with asset inventory and advances through network segmentation, intrusion detection, and ultimately risk management. The CCSPA aims high, targeting not only risk management but supply chain and third-party risk oversight. The best advice? Start where you are, and keep going.®

In his current role as Global Field CTO at Nozomi Networks, [Sandeep Lota](#) enables the success of Nozomi's sales and channel force and is both a leader and expert in executing complex design and systems engineering configurations. Having spent the first decade of his career working on the operations and project teams for global energy super-giants; Sandeep gained a powerful knowledge base of IT & OT principals which have been the foundation of his success.

How Bill C-26 Shaped Air Canada's Approach to Risk Management



Founded in 1937, Air Canada is the country's largest airline. It operates hubs in Toronto, Montreal, and Vancouver. Its fleet of more than 400 aircrafts serves 222 destinations across six continents.

When Bill C-26 (the precursor to Bill-8) was introduced in Parliament in 2022, the airline's legal team evaluated it to determine the impact it would have on the company as a transportation provider. Their evaluation quickly went to the board of directors, who agreed that the cybersecurity legislation was coming, and the company needed to prepare for it. Even though Bill C-26 never passed, that's when Air Canada began to build their program — starting with no OT security and only a vague definition of what OT assets they had.

The program consisted of four components:

- **A governance model** to guide how the security team would communicate with senior leadership and other stakeholders, from the network team to cargo managers to maintenance crews
- **An asset inventory strategy** to identify all OT assets and assess their risk

- **An OT reference architecture** for designing, securing and managing their networks

- **Incident response plans** tailored for OT

To identify the right asset inventory solution, the team conducted a three-month proof-of-value (POV), with several vendors competing apples-to-apples in critical environments that rely heavily on OT, such as hangers and cargo areas. The visibility gained from this exercise led to a key decision: categorize OT assets into two verticals. The first covers airplane control systems, including all support systems unique to aircraft. The second covers automation systems, such as safety locks, video cameras, HVAC, fire suppression, and other smart-building technologies common in airports.

During the unusually long POV, the team was able to thoroughly vet each vendor's solution and approach, picking up valuable insights that accelerated the actual implementation once a vendor was selected. In just four months, the airline deployed 35 security sensors across its operations in Canada, with more to go. Local sensors perform asset discovery, vulnerability analysis, and threat monitoring. All telemetry is then sent to the cloud for centralized monitoring, AI-powered threat analysis, profile enrichment, and risk prioritization.

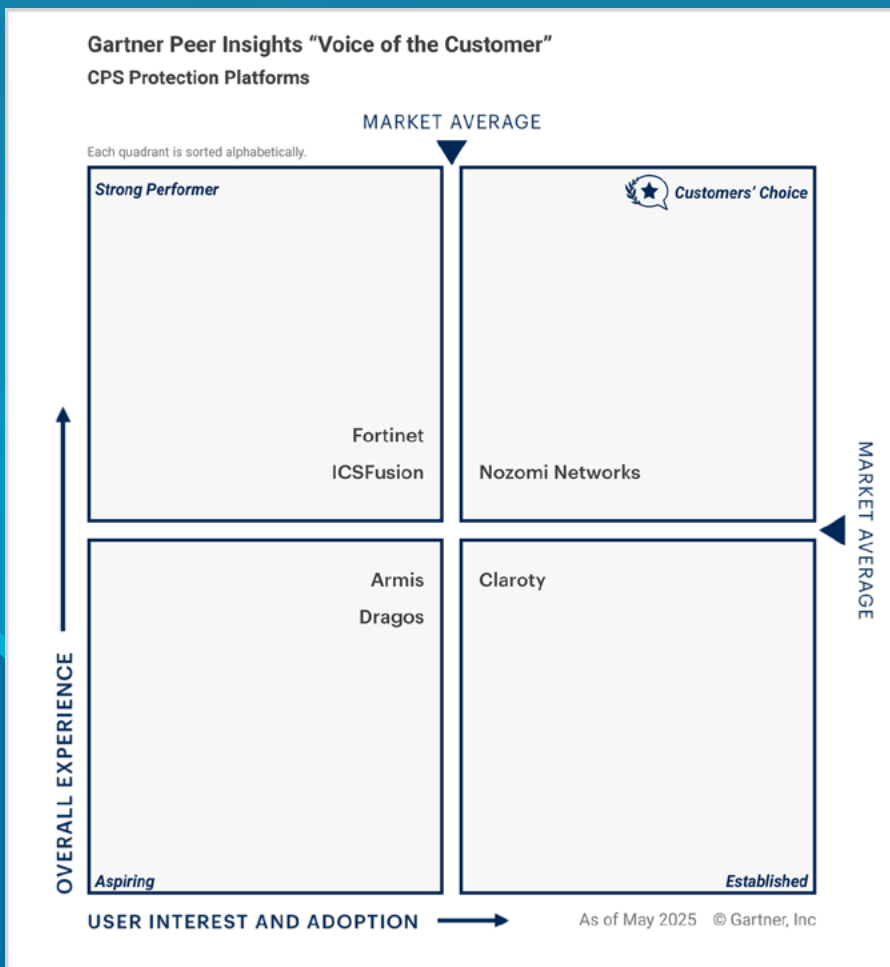
The OT security team still has plenty of work ahead of them, but with Bill C-8 still pending, Air Canada has a solid jumpstart on addressing not only the CCSPA's requirements but the company's internal goals for securing its critical cyber systems.



A Customers' Choice

See why Nozomi Networks is a Customers' Choice in the 2025 Gartner® Voice of the Customer for CPS Protection Platforms

[Download the report](#)





Secure Modernization Starts with a Map:

A planning-first approach to OT cybersecurity for SMB manufacturers

by [Juveria Khan](#)

When Modernization Outpaces Cybersecurity

Across Canada, small- and mid-sized manufacturers are modernizing. Sensors are being added to CNC machines, cloud dashboards are appearing on shop floors, and production data is feeding ERP systems, often taking place in facilities never designed for connectivity.

As digitization accelerates, cybersecurity often falls behind. In many plants, it arrives late, reactive at best and bolted on at worst. And when things go wrong in manufacturing, the impact is more than digital. It is operational, reputational, and sometimes physical.

How this challenge is understood depends on perspective. Executives focus on revenue and reputation. IT teams focus on evolving architectures, while OT teams prioritize process continuity and safety. Each view is valid, but without a shared lens, priorities pull in different directions.

Manufacturers need more than tools. They need structure that makes cybersecurity part of modernization itself. With AI accelerating both opportunities and risks, a planning-first approach provides that structure—turning cybersecurity into a guiding principle for progress rather than an afterthought.

Why Cybersecurity Struggles to Take Root

If cybersecurity is to guide modernization, manufacturers must first overcome the forces that hold it back. These forces appear again and again across SMB plants, not as technical flaws, but as recurring obstacles woven into daily operations.

OBSTACLE 1: NO ONE OWNS THE MAP

In many plants, no single role owns cybersecurity. IT manages the corporate network while OT oversees plant-floor systems. The boundaries between them are rarely mapped.

Without a baseline inventory of assets, connections, or vulnerabilities, it is impossible to know whether changes are reducing risk or simply shifting it elsewhere. Reactions are merely event-driven; an audit finding, a client requirement, or a near miss sparks activity. Effort is spent, but progress does not compound.

OBSTACLE 2: WHEN NEW MACHINES ARRIVE BEFORE SAFEGUARDS

Smart machines, remote diagnostics, and cloud dashboards often arrive faster than risks can be assessed. Production deadlines push OT to connect new systems immediately while security reviews trail behind. By the time safeguards are considered, the equipment is embedded, and retrofitting is costly.

This sequencing leaves behind hidden connections, unmanaged vendor access, and growing complexity. AI now amplifies these weaknesses by scanning for misconfigurations, pivoting across environments, and automating attack chains. Exposures that once took months to find can now be exploited in hours.

OBSTACLE 3: RISK IN DIFFERENT LANGUAGES

Executives, IT, and OT all see the same operation but prioritize risk differently.

- **For leadership:** contracts, capital, and reputation.
- **For IT:** cyber exposure and downtime.
- **For OT:** anything that threatens safety or production continuity.

Even AI is understood differently across these groups. Leadership sees headlines about disruption. IT sees new classes of malware. OT worries about manipulation of safety systems. Without a shared lens, AI risks become just another fractured conversation instead of a catalyst for alignment.

OBSTACLE 4: GUIDANCE THAT OVERWHELMS INSTEAD OF ENABLES

Standards like IEC 62443 or NIST SP 800-82 describe what “good” looks like, but they are written with large teams and mature governance in mind. For smaller manufacturers, these prescriptions often arrive as dense checklists, overwhelming teams instead of enabling action.

OBSTACLE 5: WHY GOOD ADVICE STILL FAILS

Even experienced partners can struggle when a site is not ready to absorb recommendations.

- **Tools may be deployed** without mapped boundaries
- **Reports may lack** operational paths
- **Technology may be** prioritized over team readiness

Without alignment to site realities, even sound advice fails to create lasting change.

Planning-First: A Usable Way Forward

THE URGENCY OF AI

AI is reshaping the threat landscape faster than SMBs can adapt. Larger enterprises may counter with AI-driven defenses, but smaller manufacturers cannot out-tool attackers. Their advantage lies in reducing the surface area AI-enabled attacks can exploit.

FROM AWARENESS TO ACTION

For most SMBs, the challenge is not recognizing risk—it is translating awareness into a usable way forward. Without that, initiatives misfire, vendors overshoot, and guidance struggles to take root.

GROUNDING CYBERSECURITY IN OPERATIONS

Planning-first approach transforms this challenge into progress. By rooting cybersecurity in today’s operations, it grows with modernization instead of trailing behind, creating a foundation for decisions that align people, priorities, and safeguards.

A Repeatable Framework for Progress

A planning-first approach begins with clarifying how the site operates today: what systems connect, how data flows, where boundaries exist, and which assets matter most. From this baseline, it turns into a playbook—a small set of repeatable steps that guide modernization securely, no matter the size or setup of the site.

STEP 1: START WHERE IT COUNTS

Map equipment and connections to business outcomes so the most valuable and vulnerable areas are protected first.

Example: Safeguarding the line that generates the highest revenue ensures downtime risk is minimized.

STEP 2: TRACE THE FLOW

Follow how information and control signals move across the site and out to vendors or the cloud, exposing where protection is needed most.

Example: Tracking CNC sensor data into the ERP highlights potential points of interception and alteration.

STEP 3: DRAW THE LINES

Define fit-for-site trust zones, access rules, and safeguards that align OT, IT, and business priorities without slowing production.

Example: OT maintains safety while IT manages secure vendor access, keeping operations running and risk contained.

STEP 4: KEEP IT MOVING

Build a foundation that adapts to new equipment, contracts, and regulations.

Example: When a client requires secure supplier data exchange, access rules and audit checkpoints are added to the next upgrade phase seamlessly.

Together, these outcomes turn cybersecurity planning from an abstract exercise into a practical guide that grows with the business and keeps pace with change.

Case Study: Secure Modernization in Practice

At a mid-sized equipment manufacturer, a robotic palletizer was scheduled for installation. It required vendor connectivity, data-sharing, and changes to safety protocols.

Historically:

- **OT managed deployments**
- **IT brought in late**
- **Leadership only focused** on throughput
- **Security considerations** were left for after commissioning

This time, they applied a planning-first approach:

- 1. Start Where It Counts** — OT mapped the palletizer's role in production and safety, ensuring safeguards started where downtime would be most costly.
- 2. Trace the Flow** — IT traced data flows through plant systems to vendor and cloud destinations, identifying where segmentation and monitoring were needed.
- 3. Draw the Lines** — Trust zones ensured the palletizer could operate without unfettered access to safety-critical processes. Vendor connections were authenticated, filtered, and logged from day one.
- 4. Keep It Moving** — The onboarding was documented as a repeatable template, making the next modernization faster and safer.

THE RESULT: Instead of an ad-hoc installation, the palletizer became a secure, well-integrated upgrade. It passed a client audit and left behind a roadmap for future improvements.



When Planning Comes First...

When planning comes first, SMBs unlock their real advantage: alignment. With people and priorities working from the same map, cybersecurity becomes part of how operations move forward, with:

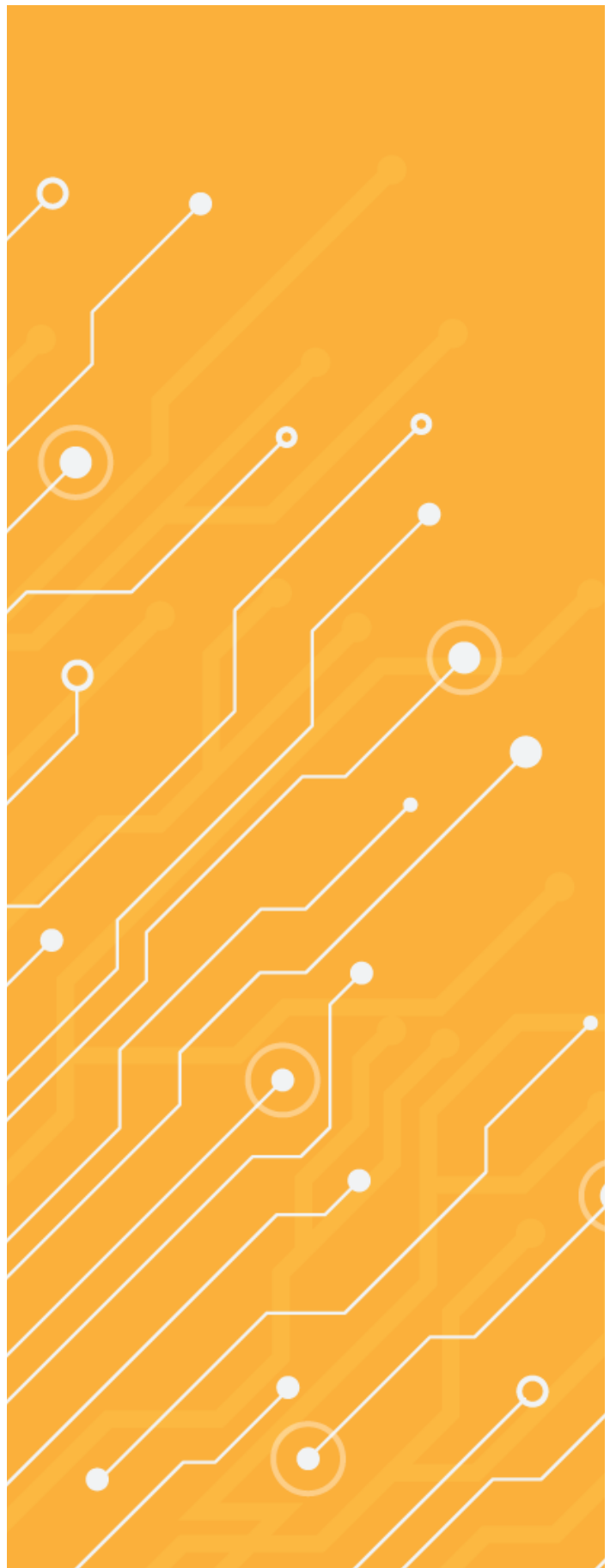
- **Clear starting points** that make action possible
- **Procurement readiness** for secure onboarding
- **Shared language** between IT, OT, and executives
- **Roadmaps aligned** with production and business cycles
- **Foundations for smoother** vendor engagement

What if cybersecurity planning could be more than a framework — a way to replace fragmentation with clarity?

Final Word

Every SMB manufacturer wants to modernize their OT environment. A Planning-First approach provides a practical launch point, but more importantly, it builds internal momentum. It empowers teams to take action without waiting for the perfect moment, the perfect hire, or the perfect tool. And that momentum, more than any policy or framework, is what makes secure modernization real. ☺

Juveria Khan is the founder of Dawn Machina, a cybersecurity company built to help small and mid-sized manufacturers prepare for secure modernization. With over a decade in IT infrastructure and more than six years managing large-scale enterprise rollouts — including Zero Trust, cybersecurity, and modernization initiatives — she brings a systems-driven lens to planning. Now advancing her expertise in engineering-grade OT security, Juveria is passionate about making cybersecurity real, practical, and accessible for SMBs, and focuses on translating industrial risk into structured, site-aware strategies to get them there.





Securing Industrial Modernization: Managing the Risks of Full Stack Convergence and AI Adoption

Presented by Xage Security and Darktrace

As digital transformation accelerates, organizations are rapidly unifying IT, OT, cloud, and industrial environments to streamline operations, boost efficiency, and gain the competitive edge. This full stack convergence marks a foundational shift—one that opens the door to unprecedented productivity and innovation across sectors like energy, manufacturing, and critical infrastructure.

But just as enterprises have begun to tackle the challenges of convergence, such as identity sprawl, lateral movement, and outdated access models—a second and far more unpredictable force has emerged: AI. The speed and scale of AI adoption introduces entirely new dynamics. Large language

models (LLMs), AI agents, and adaptive workloads are reshaping how users interact with systems, how data flows, and where decisions are made.

Together, convergence and AI represent both a breakthrough and a breaking point—offering massive opportunity but also significant risk. Traditional security tools, designed for static environments and human-driven workflows, are falling short. To move forward safely, organizations must rethink their cybersecurity foundations—starting with identity, access, and protocol-level enforcement that is enhanced by adaptive, real-time detection that is built for complexity, speed, and scale.

The Full Stack Convergence Imperative

Industries are accelerating digital transformation to drive greater performance, resilience, and efficiency. At the heart of this evolution lies full stack convergence—the unification of IT, OT, cloud, IoT, and IIoT systems into a single, cohesive operational ecosystem. This convergence is a force

With greater connectivity comes greater exposure.

multiplier, enabling everything from smart grids and intelligent energy storage to remote automation, edge computing, and adaptive manufacturing.

But with greater connectivity comes greater exposure.

Convergence Risks

Legacy OT systems were never intended to be connected. Designed for uptime, not cybersecurity, they often lack basic safeguards like encryption, authentication, or endpoint protection. Many can't host agents or receive timely patches, leaving them defenseless in the face of modern threats. When paired with blunt tools like VPNs, which grant broad access without enforcing protocol-level controls, these environments become dangerously overexposed.

Managing access across such a heterogeneous landscape is equally challenging. Different asset types often rely on incompatible identity systems, making it difficult to govern access consistently—especially for third parties like contractors, vendors, or service technicians. Without unified identity and access management, enforcing least-privilege becomes impossible, and unauthorized actions go unchecked.

Lateral movement compounds the risk. Firewall-based segmentation, while necessary, is often manual and error-prone. Static rules can't adapt to dynamic workflows, and attackers exploit these gaps to move between systems undetected. The problem is exacerbated by visibility silos: most monitoring tools are designed for IT or OT, but not both—making real-time detection and response across domains slow and incomplete.

What is required instead is passive, agentless network monitoring that spans IT and OT protocols, providing organizations with a unified operational picture. This enables anomaly-based threat detection and behavioral analytics that can surface malicious activity such as credential misuse, insider threats, or “living off the land” tactics, before attackers reach critical assets.

Meanwhile, the threat landscape continues to escalate. Ransomware and insider attacks increasingly target industrial systems, exploiting credential misuse and configuration blind spots. Insiders with valid access can bypass traditional perimeter defenses, while attackers who compromise a single credential can pivot rapidly, especially if session activity isn't properly contained.

For years, these challenges gave organizations reason to delay convergence efforts. But postponement is no longer an option. The organizations that wait are falling behind, operationally and competitively. And even as they begin to integrate their stacks, a new and more volatile force is already reshaping the landscape.

That force is AI. And while it promises extraordinary capability, it introduces a new class of risk—one that legacy tools simply weren't built to handle.

AI Has Arrived—Ready or Not

While full stack convergence has been unfolding over the past decade, the rise of AI has been far more sudden and disruptive. From natural language models and AI agents to predictive analytics and autonomous systems, AI is reshaping every sector. Industrial environments like energy and defense are among the early adopters. What began with convergence, AI is now accelerating at exponential speed.

AI holds immense promise: boosting employee productivity, automating complex tasks, extracting value from massive datasets, and predicting operational needs like maintenance or optimization. The innovation potential is undeniable.

But so is the risk.

Employees are using AI tools to solve real problems regardless of official policy.

Organizations are eager to embrace AI but hesitant to unleash it without clear guardrails. Security and business leaders understand the stakes. Unlike the managed rollout of convergence, AI has already entered the enterprise, often through grassroots adoption.

Employees are using AI tools to solve real problems regardless of official policy. That means organizations no longer get to choose if AI is part of their environment; they must now decide how to secure it.

Why AI is Hard to Secure

Securing AI is not simply a matter of applying traditional controls. AI systems are dynamic, distributed, and multi-layered—spanning models, agents, APIs, data sources, compute infrastructure, and external services. These components often operate across internal data centers, cloud platforms, and partner ecosystems, involving a wide array of users and access patterns.

Unlike conventional systems, AI introduces many-to-many interactions: users interact with agents, agents communicate with LLMs, LLMs retrieve or generate data—all in real time. These shifting relationships defy static rules and perimeter-based

security models. Legacy tools simply can't monitor or govern such decentralized, adaptive workflows.

One of the most pressing risks is AI jailbreaks—when users, whether malicious or just curious, manipulate AI prompts to bypass safety restrictions and gain unauthorized access. These attacks exploit the fluid nature of language and logic in LLMs to retrieve sensitive data, generate harmful outputs, or execute unintended actions.

This complexity creates a fragile security posture. A single blind spot like a misconfiguration, an over-permissioned identity, or an unchecked API call can trigger cascading consequences: lateral movement, data leakage, reputational damage, regulatory exposure, or operational disruption.

This is where adaptive, self-learning security becomes essential. Passive network monitoring and anomaly-based detection continuously baseline system behavior across IT and OT, rapidly surfacing unexpected or high-risk activity—even when it doesn't match known attack patterns. Combined with protocol-level access enforcement, it ensures AI adoption does not outpace the organization's ability to secure it.

Building Security That Understands Industrial Complexity

As industries modernize through full stack convergence and AI adoption, security must evolve alongside them. Yet too often, cybersecurity is applied as an afterthought, bolted on in a piecemeal fashion rather than built into the foundation. The result? Fragmented protection, inconsistent controls, and significant exposure across critical systems. To unlock the full potential of modern technologies, and avoid their unintended consequences, organizations must adopt security solutions that are purpose-built for industrial complexity.

An effective strategy must balance two equally vital pillars: Protection & Prevention, and Detection & Response. While each plays a distinct role, their impact is amplified when operating as a unified system.

Protection & Prevention

Modern threats target the weakest link, often not the system itself, but rather identities, sessions, tokens, and credentials. That's why security must shift from infrastructure-centric to identity-centric models of protection.

For converged environments, protection starts with an extensible platform that delivers end-to-end enforcement across IT, OT, cloud, and data center layers. This includes integrated capabilities such as Secure Remote Access (SRA), Privileged Access Management (PAM), network segmentation, and fine-grained access control—all working in unison to eliminate blind spots and enforce Zero Trust across environments.

To be resilient, this foundation must support:

- Quantum-safe encryption
- Phishing-resistant MFA
- Tamperproof enforcement
- Adaptive authentication
- High availability, even under attack or system failure

When it comes to AI, traditional defenses are no longer sufficient. LLMs and AI agents must be protected not only from external threats but also from internal misuse, whether intentional or accidental. This requires jail-break-resistant, protocol-level enforcement (e.g., MCP, A2A), where access to sensitive data is governed at the protocol layer, independent of how the AI behaves. This approach ensures that AI systems can't be manipulated into leaking or misusing data through prompt-based attacks.

Detection & Visualization

Why detection still matters: Even the strongest preventative controls cannot eliminate every risk. In converged and AI-driven environments, there

will always be blind spots, misconfigurations, or insider activity that slip through. This makes advanced detection and rich visualization capabilities indispensable for resilience.

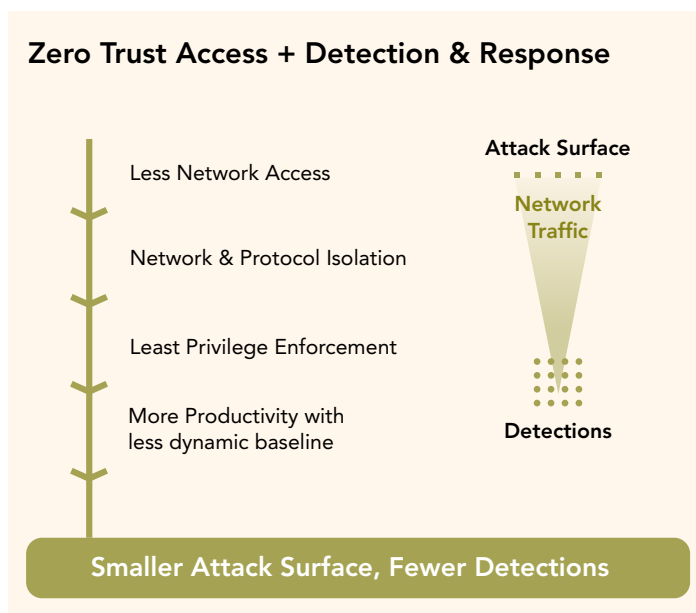
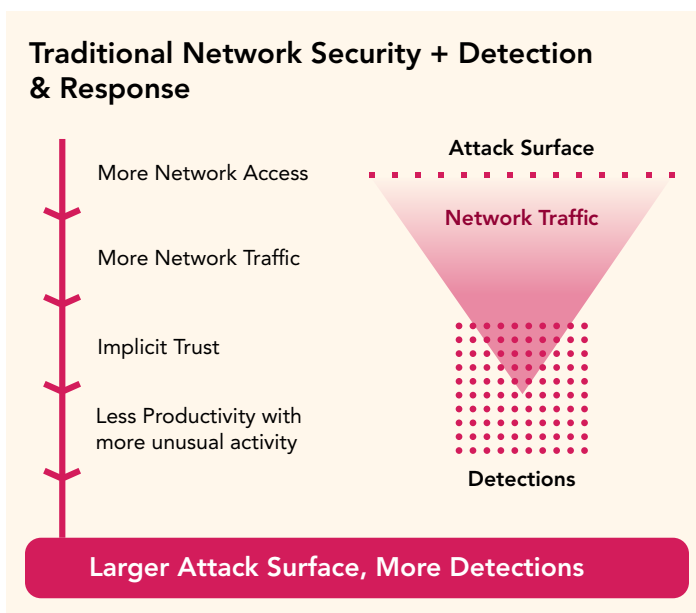
The limits of legacy approaches are increasingly evident. Detection built on signatures, static rules, or perimeter-only monitoring struggles to keep pace with the fluidity of modern industrial systems. Adversaries now rely on subtle tactics such as abusing valid credentials, blending into normal workflows, or exploiting trusted insiders. These “living off the land” techniques evade rule-based detection, creating long dwell times before discovery.

Modern detection requires an adaptive, self-learning AI approach. By continuously tuning its understanding of what “normal” looks like across IT and OT networks, the system adapts in real time to shifting environments. This ensures that even never-before-seen threats, such as abnormal user activity, misused identities, or AI models behaving unexpectedly, are surfaced immediately.

Equally critical is the visualization of attack paths. Raw alerts alone do not reveal how an intrusion might spread. Mapping relationships across IT and OT provides analysts with a dynamic picture of how lateral movement could unfold. Seeing the chain of potential escalation, from a compromised credential in IT to a PLC in OT, enables defenders to intervene early—all before operations are impacted.

Prioritization also defines effective detection. Instead of overwhelming analysts with an indiscriminate flood of low-value anomalies, modern systems elevate the events that matter most, such as insider misuse or compromised privileged accounts. This reduces noise, combats alert fatigue, and keeps security teams focused on genuine risks.

Finally, identity-contextual visibility is indispensable. By correlating behavior with human and machine identities in real time, organizations achieve a deeper understanding of who is doing what, when, and why. This identity-centric lens accelerates investigation, reduces



mean-time-to-detect, and enables faster, more accurate response when incidents occur.

The outcome is a shift from indicators to insight. Rather than chasing yesterday's indicators of compromise, organizations continuously learn from today's environment. By unifying IT and OT visibility, embedding self-learning AI, visualizing lateral movement, prioritizing risk-based alerts, and enforcing identity-driven context, enterprises can dramatically reduce cyber risk at scale, securing industrial modernization without sacrificing speed or innovation.

Better Together: A Unified Defense

Independently, prevention and detection provide value. But when combined into a single, coordinated strategy, they form a force multiplier.

Preventative controls reduce unnecessary network traffic and lateral movement, which improves detection system efficiency. This results in fewer, higher-confidence alerts that are easier for security teams to manage, helping to combat alert fatigue and ensuring that focus remains on genuine threats.

In the era of full stack convergence and ubiquitous AI, the stakes are higher and the margin for error is narrower. Fragmented approaches can't keep up. A unified security architecture that is built on identity, enforced at the protocol level, and enhanced by AI, will be essential to protecting against both malicious actors and the unintended consequences of emerging technologies.

Conclusion

The convergence of IT, OT, and cloud infrastructure has redefined the boundaries of enterprise security. The rise of AI has shattered them entirely. Together, these forces represent the most significant transformation, and the greatest challenge that industrial organizations have ever faced. Legacy tools and piecemeal approaches are no longer sufficient. To move forward safely, organizations must embrace a new security paradigm: one that is identity-centric, protocol-enforced, and built for continuous adaptation.

Protection and prevention must go hand in hand with detection and response. Only by unifying these capabilities can enterprises reduce their attack surface, enforce least privilege, and respond to threats before damage is done. This is not just a matter of compliance or hygiene, it's a matter of resilience, operational continuity, and long-term competitiveness.

Organizations that succeed in securing convergence and AI adoption will not only safeguard their environments, they'll unlock new opportunities for innovation, automation, and leadership in the digital era.🔒

Modernize Securely. Operate Fearlessly.

Unleash the potential of AI—without
fearing what it might do next.

With the right security foundation, AI becomes a driver of innovation, not a source of risk. Protect your data. Control access. Detect threats before they cause damage.

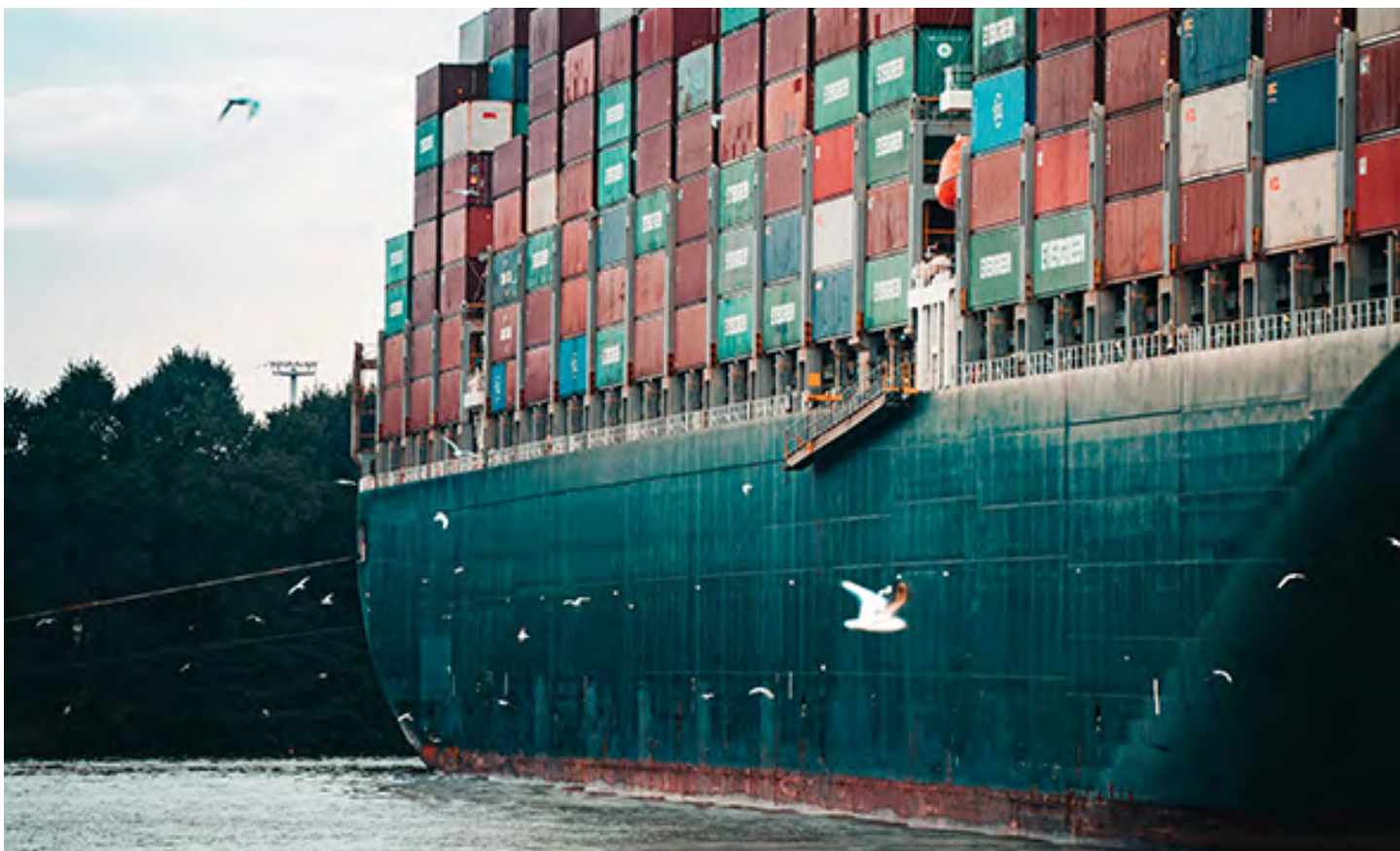


xage
SECURITY



DARKTRACE

www.xage.com | www.darktrace.com



Reproducible Builds and Full-Source Bootstrapping

by [Anton Livaja](#)

Sunburst: A wake-up call for supply chain security

In 2020, the industry was in disbelief when SolarWinds was targeted in what was one of the boldest software supply chain attacks on record. Attackers had successfully injected malware into the Orion IT management software update, which was then distributed to as many as 18,000 customers worldwide. Victims included Fortune 500 companies, government agencies, and critical infrastructure operators.

The breach, codenamed “Sunburst”, exposed a chilling truth about third-party software: even a signed software update from a leading cybersecurity vendor can become

a Trojan horse. This report examines the systemic trust failures that enabled the breach and the safeguards that can prevent this type of compromise.

Trusting trust: The compiler backdoor problem

The SolarWinds saga evokes a prescient warning from 1984, when Ken Thompson, co-creator of Unix, published his seminal essay, *Reflections on Trusting Trust*. Thompson argued that you can’t trust a program just because you wrote its source code. He demonstrated how a skilled attacker could plant a backdoor not in the source itself, but in the compiler used to build it.

In other words, even if a thorough review finds no malicious instructions, a compromised compiler could silently inject malware each time it compiles the program. This idea was weaponized long before Sunburst, most notably during the 2015 [XcodeGhost](#) incident. In that case, developers unknowingly used a tainted version of Apple's Xcode compiler, which injected backdoors into applications built from clean source code. The result was thousands of compromised iOS apps, used to exfiltrate data from infected devices. Of course, this risk extends to other means of manipulating the environments in which software is built, and run.

Reproducible Builds: Determinism as a Defense

A powerful approach to reducing supply chain risk is the use of reproducible builds. Also known as deterministic builds, this software building method guarantees that the same source code will always produce identical binaries bit-for-bit, regardless of where or when code is built. The security benefit is significant. When independent parties compile software from source in isolated environments and produce identical outputs, any unauthorized changes, including malware injection, become immediately detectable.

A powerful approach to reducing supply chain risk is the use of reproducible builds.

Reproducible builds transform the software pipeline into a verifiable process. While monitoring can be an effective strategy for gathering information about what's happening in a given context, it has no ability to say anything about the integrity of software once it leaves that context. SolarWinds had significant monitoring measures, but no way to verify integrity of software outside of that, a gap that proved costly for both the company and its clients.

For reproducibility to be effective, the systems performing these builds must be diverse, varying in access controls, hardware, firmware, and operating systems, to reduce the risk of being compromised in the same way. In contrast, non-deterministic builds lack even the basic ability to verify integrity once the code leaves the pipeline. In other words, *security through diversity*, is a powerful idea that can be applied, not only here but across systems in different contexts.

SolarWinds acknowledged the short comings of relying solely on monitoring in their post-breach report, [Setting the New Standard in Secure Software Development](#). In it, it was noted that reproducible builds could have been an effective safeguard against the Sunburst malware, a method that might have detected unauthorized changes before deployment.

Full-Source Bootstrapping: Eliminating Hidden Seeds of Compromise

Reproducible builds assume that the compiling tools are trustworthy. Full-source bootstrapping takes this a step further by ensuring that software is built from fully verifiable source code. It omits any precompiled binaries, which can conceal malicious behavior and are difficult to inspect. To sufficiently eliminate risk stemming from this attack vector, the entire software supply chain should be constructed in this manner—without relying on opaque binary “seeds.” The comprehensive approach starts from a minimal, verifiable binary (e.g., a tiny hand-written compiler), bootstrapping the entire modern toolchain in a reproducible manner. The result is a fully transparent stack where every component can be traced to source.

Reproducibility and bootstrapping must be employed together to meaningfully reduce the risk Thompson described.

Challenges with Closed-Source Software

Proprietary systems remain black boxes—making it impossible to independently verify their security or integrity. Organizations with proprietary software can use reproducibility to improve internal supply chains, but end users cannot independently verify the software until it is open source. This forces organizations to rely on trust alone, a weakness that sophisticated adversaries have already exploited. The [Stuxnet malware](#), for example, hijacked legitimate code-signing certificates to deliver its payload undetected. Organizations operating in high-risk environments should demand reproducibility and

transparency from vendors and shift toward open source alternatives where possible.

Building a Trustworthy Software Ecosystem

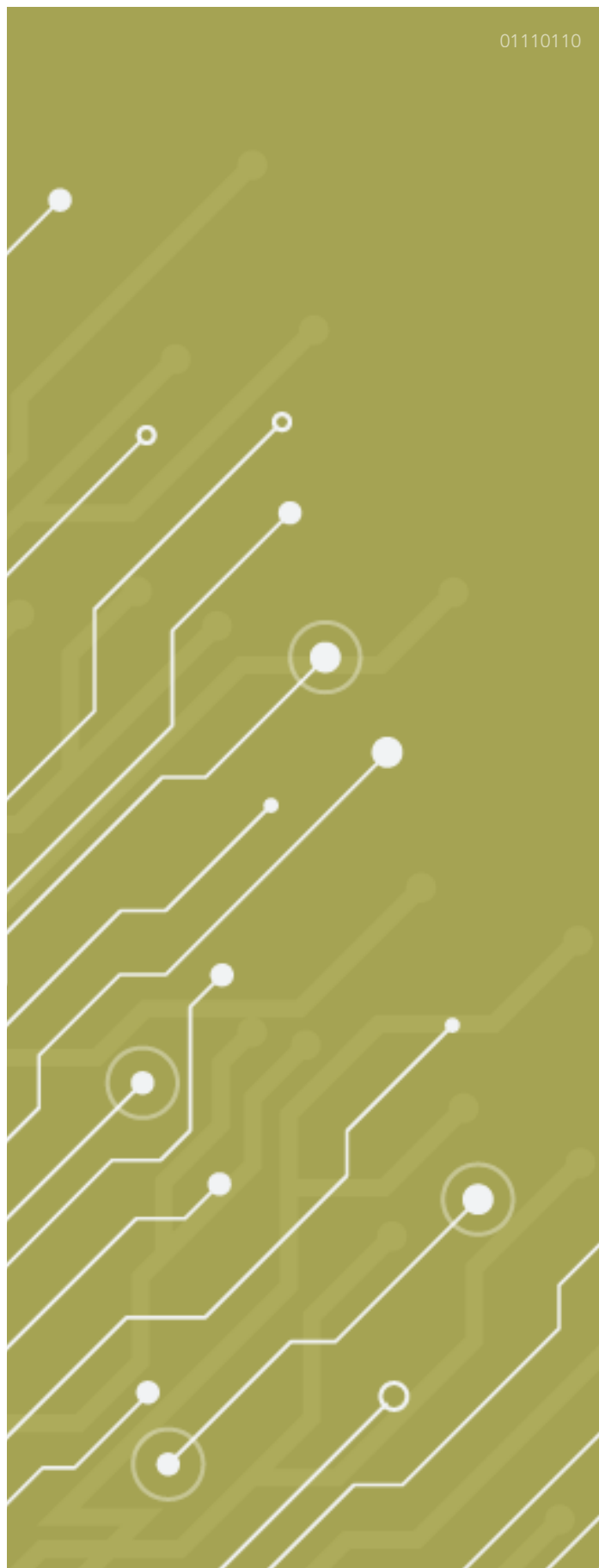
For CISOs and leaders in OT and critical infrastructure, the time to act is now. Key steps to building a trustworthy ecosystem include:

- **Adopting reproducible build** pipelines and use fully source-bootstrapped software internally
- **Choosing vendors who publish** source code and build instructions, and those who follow reproducible, source-bootstrapped processes
- **Manually reviewing all code**, including third party components for weaknesses, and ensure it can be independently reproduced

The industry must move beyond assuming software, or firmware, is secure simply because it's signed or comes from a "trusted" vendor. Instead, adopt a healthy level of distrust and prioritize verifiability at every layer of the stack. SolarWinds' compromise made it painfully clear, *trust without verification is a vulnerability*. By embracing reproducible builds and full-source bootstrapping, we can move a step closer to establishing a transparent foundation for the software that powers critical infrastructure and strengthens national resilience.®

Anton Livaja is a security engineer specializing in the design of high-assurance systems which can withstand even the most adversarial environments. With expertise spanning applied cryptography, confidential and verifiable computing, distributed systems, and supply chain security, he has architected vaulting and custody solutions protecting over \$100 billion in digital and financial assets across global financial institutions, cryptocurrency platforms, and critical infrastructure operators.

Renowned for eliminating single points of failure and embedding resilience at every layer, Anton delivers security architectures that withstand both sophisticated cyber threats and systemic disruptions. His mission is to advance freedom, privacy, and security worldwide by addressing the most fundamental and complex challenges in the field. To this end, Anton co-founded two security firms, Distrust.co and Caution.co.





The Evolving Operational Technology (OT) Security Landscape

by [Jason Grimbeek](#), Presented by Iron Spear Information Security

OT systems are the backbone of industrial operations, from manufacturing and transportation to energy and utilities. Historically isolated, these systems are now increasingly connected to enterprise IT networks, cloud platforms, and remote access tools. This convergence has unlocked new efficiencies, but it has also introduced significant cybersecurity risks.

Recent attacks on critical infrastructure have demonstrated that OT environments are no longer immune to cyber threats. Ransomware incidents have shut down production lines, disrupted energy grids, and compromised safety systems. Regulatory frameworks such as NIST CSF 2.0, IEC 62443, and NERC CIP are pushing organizations to adopt

structured approaches to OT cybersecurity. But compliance alone isn't enough. Organizations need pragmatic, risk-based strategies that align with operational realities and business priorities.

Contemporary OT Security Challenges

LEGACY SYSTEMS AND TECHNICAL DEBT

Many OT environments rely on legacy equipment that was never designed with cybersecurity in mind. Protocols like Modbus, DNP3, and BACnet lack encryption and authentication, making them vulnerable to interception and manipulation. These systems often run outdated firmware and

cannot be patched without disrupting operations. In most cases, they have little or no capacity to apply security controls, let alone integrate with modern off-the-shelf security solutions for OT. Many of these legacy systems are proprietary, and the workforce that can support them is aging.

VISIBILITY AND ASSET INVENTORY

A foundational challenge in OT security is the lack of visibility. Many organizations lack a complete inventory of their OT assets, including controllers, sensors, HMIs, and networked devices. Shadow OT, unauthorized or undocumented devices, can proliferate in large environments, especially when changes are made without centralized oversight.

A foundational challenge in OT security is the lack of **visibility**.

Traditional IT asset discovery tools are often unsuitable for OT environments. Active scanning can disrupt sensitive systems and doesn't typically work in heterogeneous environments where vendors from different generations use disparate protocols. About 60% of the environments we see lack a complete picture of their industrial networks. While some veteran engineers and technicians have deep knowledge of what is there, it is in their heads, often, their perception of what is there differs from reality. Spreadsheets are the most common mechanism to maintain the asset inventories, yet fewer than 20% are maintained 6 months after implementation. Passive monitoring tools tailored for industrial protocols are essential but underutilized.

IT/OT INTEGRATION RISKS

In Canada, the energy, utilities, and larger industrial sectors have largely kept the IT and OT worlds separate. Smaller environments, often manufacturing organizations, are more likely to integrate the two. This integration is being driven by business needs for data, while initiatives such as

Industry 4.0 and Industrial Internet of Things (IIoT) deliver significant benefits and efficiencies, they also greatly expand the attack surface.

OT is built around flat network architectures, shared credentials, and poorly defined trust boundaries, allowing attackers to move laterally from IT systems into OT environments. The lack of segmentation means that a single compromised device can impact an entire production line.

Moreover, IT security policies may not translate well to OT environments, where uptime and safety take precedence over patching and updates. This misalignment can lead to gaps in protection and response. OT teams typically don't trust their IT counterparts, as they lack understanding of the plant floor. Conversely, IT sees OT as resistant to modernization and efficiency.

CYBERSECURITY SKILLS GAP

Canada's vast geography means many industrial plants are located in remote areas. Staffing for skilled instrument technicians and engineers is already a problem, let alone skillsets in OT cybersecurity; the shortage of such expertise is significant. Many IT cybersecurity consultants struggle in these environments because they lack the operational perspective where the primary concern is uptime and safety, as well as the specialized knowledge of industrial processes, protocols, and equipment. On the other hand, OT engineers typically do not have deep expertise in networking, let alone advanced cybersecurity capabilities.

CANADIAN REGULATORY LANDSCAPE

Canada has historically been slow to implement comprehensive federal cybersecurity legislation, especially when compared to its G7 and EU peers. While some provinces have taken proactive steps, such as Alberta's Security Management for Critical Infrastructure Regulation, which came into force in May 2025 and mandates CSA Z246.1 compliance for critical infrastructure. The federal government has struggled to pass national cybersecurity laws with meaningful enforcement mechanisms.

The most recent effort, Bill C-8, was introduced in June 2025 and is currently at second reading in the House of Commons. It aims to establish the Critical Cyber Systems Protection Act (CCSPA), which would impose mandatory cybersecurity obligations on operators of vital infrastructure sectors, such as telecommunications, energy, transportation, and banking. However, this bill is nearly identical to Bill C-26, which was first tabled 2022 but failed to pass when Parliament was prorogued in early 2025. As a result, Canada is effectively restarting the legislative process while

other nations and jurisdictions have already advanced their cybersecurity frameworks.

In contrast:

- **The United States** has implemented sector-specific mandates through agencies like CISA and NERC, and introduced binding directives for critical infrastructure operators.
- **The European Union** has enforced the NIS2 Directive, requiring all member states to transpose cybersecurity obligations into national law by October 2024, with strict penalties for non-compliance.
- **The United Kingdom**, the Data Use and Access Act (DUAA) received Royal Assent in June 2025. While not a dedicated cybersecurity law, it updates the country's cybersecurity and data protection framework to address emerging threats.

Canada's delay has created uncertainty for businesses operating in federally regulated sectors. While Bill C-8 is expected to advance due to strong government support, its scope is narrow. The lack of a consistent and enforceable federal framework means that many organizations resort to provincial guidance or voluntary standards, which ultimately rely on best efforts.

Pragmatic Strategies for OT Security

ESTABLISH A UNIFIED GOVERNANCE MODEL

Effective OT security requires collaboration across IT, OT, and cybersecurity teams. Define clear roles, responsibilities, and escalation paths. Establish governance structures that align with industry frameworks like NIST CSF 2.0 and IEC 62443, and ensure that OT security is represented in enterprise risk management.

Encouragingly, 52% of organizations now place OT cybersecurity under the CISO or CSO, up from just 16% in 2022 (according to Nozomi's OT/IoT Security Report 2025). This shift reflects growing recognition that OT security is a strategic, enterprise-wide concern.

OT requires cybersecurity standards tailored to its environment, as IT standards often fail to address its challenges. While some overlap exists, OT programs must align with relevant industry frameworks. We recommend starting with basic compliance; aiming for the highest level immediately is usually unrealistic. Focus on achievable goals to build momentum and trust before pursuing further advancements.

STRENGTHEN KEY CONTROLS

- **Network Perimeters** – Knowing exactly what is coming in and going out of the network is critical. These should be checked every 90 days. Traffic entering the network should be limited to strict conditions and approvals.
- **Accurate Asset Inventory** – Without understanding what is there, organizations will never know what shouldn't be there. Additionally, an accurate register tied to active threat intelligence will enable a true understanding of risk.
- **Physical and Logical Access** – Move away from shared accounts where possible, and when they are used, make use of physical controls to restrict who can use those consoles. Unlocked cabinets or HMIs are often left in rarely accessed areas, with credentials posted on the screen.
- **Secure Remote Access** – When required, remote access should be adequately secured. Do not rely solely on the corporate remote access security systems; there should be a secondary mechanism to validate who is entering the control networks.
- **Malware protection and OT-aware intrusion detection systems (IDS)** – Malware, be it ransomware or something just as sinister, will cripple most plants. While the data itself rarely justifies paying a ransom, the real cost lies in the time needed to restore operations, which impacts the bottom line. Most systems will take a minimum of 48 hours to get back to basic operations after a serious malware event.
- **Cyber Resilience** – Cyber resilience is critical and not well understood in the OT space. It is facing the reality that something will happen at some point, and ensuring your network is ready to recover as fast and painlessly as possible. This is done through the following:
 - » **Backups** – Ensuring backups for critical configurations and systems that cannot be restored from scratch. These backups should be protected from any possible malware attack, too, kept offline or in immutable vaults/storage.
 - » **Redundant Hardware** – Too many times, we see plants with limited spare parts for the OT systems. Organizations rarely spend the effort to truly understand which OT components are critical and determine how long in reality it would take to replace them. In some cases, single-core switches supporting DCS systems in remote regions of Canada are not backed up, with the assumption that new units can

simply be purchased and reconfigured. Getting a core switch in Northern BC is not typically a same-day service; they would have to be flown in from Calgary or Vancouver, assuming the supplier has stock. The result can be a minimum of 48 hours of lost production, all because the business didn't understand the cost of replacement inventory versus the loss of production.

» **Incident Response** – An OT cyber event is unique from IT, and OT environments will need unique playbooks on how to handle them before the corporate cyber teams can assist. Cyber incident response plans are vital and should be tested annually to get everyone in the know and well-versed with what could transpire during a major event.

- **Education and Awareness** – Plant environments are different from IT, engineers, operators, and technicians should understand what a cyber attack could look like and what the important risks are, such as the use of USB devices and leaving closet doors unlocked.

Looking Ahead: Building Cyber into the Future of OT

OT environments have been static by nature; very seldom do we see upgrades annually or new technology introduced as it is released. We have seen some plants with technology that dates to the 70s, still operated by aging staff. Younger employees, meanwhile, are frustrated at not seeing newer technologies. As this landscape evolves, we have to think ahead. The days of saying OT will never change are gone; businesses want more data for near real-time analytics, and staff reductions highlight the need for automation and remote access. Cloud-native SCADA platforms are gaining traction as organizations seek to centralize operations, reduce overhead and enable remote access.

Industry 4.0 is transforming manufacturing and industrial processes through digital technologies. It is bringing the evolution of “smart factories” to the frontline where people, machines, and systems all communicate and collaborate in real-time, leading to higher efficiency, flexibility and specialization. This will require faster decision-making, by using machine learning or feeding real-time data outside of the production floor.

OT Cybersecurity must play a leading role in guiding decisions on adopting new technologies and processes that enable these changes. It is essential that companies establish robust OT cyber programs to manage the changing risk landscape.

ADOPTING CHANGE AS THE NORM IN OT

Like it or not, industrial systems are evolving fast, and we will see AI playing a larger role in process control. But with these new technologies comes the requirement to interact with external networks. As organizations, we need to look forward and architect our environments for change. This won't happen overnight, but it's significantly more work to do a full change in 10 years rather than incrementally over that time. OT security programs need to be ready for this change and introduce the right amount of control as it evolves. Trying to bolt security onto a new environment is near-impossible and will only mimic what is currently in place with the current outdated environments.

Industry 4.0 is transforming manufacturing and industrial processes through digital technologies.

EMBRACING ZERO TRUST PRINCIPLES IN OT

Zero Trust is gaining traction in OT environments. It involves continuously verifying identities, enforcing least privilege, and segmenting networks to minimize trust zones. Controllers in one segment of the network typically have no reason to talk to controllers in other parts of the plant.

LEVERAGING AI/MACHINE LEARNING FOR PREDICTIVE MAINTENANCE AND ANOMALY DETECTION

Machine learning can help detect subtle deviations in system behaviour, often before a failure or breach occurs. These tools can enhance both cybersecurity and operational efficiency. As AI evolves, we cannot ignore the potential benefits it will bring to industrial processing. Organizations need to be ready to secure the environment when it does come.

THE ROLE OF DIGITAL TWINS IN PROACTIVE RISK MODELLING

Digital twins, virtual replicas of physical systems, can simulate the impact of cyberattacks or misconfigurations. Adopting these enables proactive risk assessment, scenario planning, and training in otherwise sensitive systems that cannot be tinkered with.

UPSKILLING THE WORKFORCE FOR INTEGRATED IT/OT SECURITY

People are the first line of defence. Cross-train engineers and operators on cybersecurity fundamentals. Develop hybrid roles that understand both process control and digital risk. Encourage certifications like GICSP, ISA/IEC 62443, and CISSP, and provide hands-on labs and simulations.

For larger organizations, consider establishing a dedicated OT security role or team to set standards and provide centralized guidance. Engage qualified external partners to support incident response (when and where needed) and surge capacity during emergencies.

Conclusion

Planning cybersecurity for OT over the next 10 years requires a forward-thinking and adaptive strategy, given the rapid evolution of threats, technology, and regulations. There will be a sizable shift in technology use in most industries, and security will need to be at the forefront. The silos between IT and OT will start to fade as the technology melds together. We need a dynamic approach to risk that incorporates real-time threats and vulnerabilities, as well as changes in the OT environment. Supply chain security is critical and will only become more important as cloud-enabled systems come online for the industrial sector. Organizations need to start the paradigm shift now in their OT cyber programs, as the rate of technology adoption in the industrial sector will be fast.®

Jason Grimbeek is the CEO of Iron Spear Information Security Ltd., a renowned Canadian cybersecurity firm specializing in OT and industrial systems. With over 25 years of experience in information security consulting and auditing, Jason has spearheaded projects across five continents in critical infrastructure sectors such as power utilities, transportation, mining operations, oil and gas, and aviation.

As a qualified engineer, Jason possesses a deep understanding of the unique challenges within OT environments, allowing his team to devise practical solutions that meet security requirements beyond standard audit recommendations. Recognized in the industry for his pragmatic approach to cybersecurity in both industrial and business contexts, Jason excels in communicating complex issues to both technical and executive teams. This skill has positioned him and Iron Spear at the forefront of guiding numerous organizations in developing their cybersecurity programs.

INDUSTRIAL CYBERSECURITY CONSULTING,

Minus the Sales Pitch!

Cybersecurity for industrial environments should be about **protecting critical operations**, not pushing products. At **Iron Spear**, we take a **partnership-first approach** — grounded in expertise, transparency, and real-world experience securing **OT and ICS environments**.

Here's how we do things differently:

- **No sales teams.** You work directly with **cybersecurity professionals** — not someone trying to meet a quota.
- **No vendor affiliations.** Our advice is **technology-agnostic**, driven by what's right for your control environment — not what earns us a commission.
- **Operationally practical solutions.** Industrial cybersecurity isn't only about checking boxes — it's about **safe, effective defences** that account for uptime, legacy systems, and safety-critical processes.
- **Community-first mindset.** We believe in giving back — through volunteering, sponsoring security events like BSides, and offering bursaries to support emerging talent.

We're here to help you navigate the complex world of industrial cybersecurity with **honest, actionable guidance** — so you can keep your operations safe, resilient, and focused on what matters most.

- Find us online:
WWW.IRONSPEAR.CA





The Human Impact of OT Failures

by [François Guay](#)

Operational technology (OT) systems power the critical infrastructure we rely on every day, from hospitals and power grids to water treatment and transportation networks. When these systems fail or fall victim to cyberattacks, the consequences are no longer just technical glitches; they are disruptions that can harm lives and livelihoods. In recent years, Canada and countries worldwide have witnessed OT failures that delayed surgeries, caused blackouts, and put public safety at risk. The following article explores how such incidents in various sectors have real human impacts, and why OT security must be seen as a public safety imperative rather than just a tech issue.

Hospitals Under Siege: Cyberattacks Putting Patients at Risk

Perhaps nowhere is the human cost of an OT failure more immediate than in healthcare. Modern hospitals rely on networked medical devices, electronic health records, and scheduling systems, all part of their operational technology. When a cyberattack cripples these systems, critical care can grind to a halt. In late 2023, a stark example unfolded when five hospitals in southwestern Ontario were hit by a ransomware attack via their IT provider. The attack shut down hospital email, Wi-Fi, and patient information systems, forcing staff to revert to pen and paper to track patients. Surgeries, including cancer treatments, were

postponed as hospitals scrambled to manage care using manual, backup procedures. “Cancer treatment is being cancelled. Surgeries are being postponed. Our patients are hurting... this attack has resulted in actual pain and suffering,” one Ontario hospital official pleaded in a message to the attackers (La Grassa 2023). This chilling statement underscores that when hospital OT fails, it directly translates to human suffering.

Canada has faced similar crises before. In Newfoundland and Labrador, a 2021 ransomware attack collapsed much of the province’s health network. Widespread IT outages hit on October 30, 2021, forcing doctors and nurses at the St. John’s hospital to keep records by hand. Thousands of appointments including cancer care were canceled as officials struggled to restore systems. Patients requiring diagnostic scans, lab tests, or elective surgeries saw their care delayed for weeks. An investigation later revealed that the personal health data of nearly the entire province had been compromised. More tragically, in Germany, a ransomware attack in September 2020 forced Düsseldorf University Hospital offline, leading to a critically ill patient being diverted 32 km away for care (Silomon 2020; O’Neill 2020). The delay of about one hour proved fatal. Prosecutors called it the first suspected death ‘by ransomware,’ after the hospital’s digital coordination systems were paralyzed and hundreds of operations were canceled. While it remains difficult to conclusively pin a death on a cyberattack, these cases show that disrupted OT in hospitals can literally become a matter of life or death.

Even when lives aren’t lost, the quality of care suffers during such incidents. When Toronto’s Hospital for Sick Children (SickKids) was hit by ransomware in December 2022, clinicians lost access to critical digital tools. Lab and imaging results were delayed, leading to longer wait times for patients and families, despite the limited number of systems that were encrypted. For parents in the pediatric hospital, those delays in diagnosis and treatment added anguish to an already stressful time. Across the board, health workers report feeling immense stress as they struggle to deliver care without functioning IT, while patients endure uncertainty and postponed treatments. Each of these stories, canceled cancer treatments, delayed surgeries, frantic emergency diversions, highlights the human toll when hospital OT fails.

Power and Energy: Blackouts in the Modern Dark Age

The impacts of an OT failure in the energy sector are immediately felt in homes and businesses. An infamous example was the May 2021 Colonial Pipeline ransomware attack in the United States, which prompted the operator to shut

down a 5,500-mile fuel pipeline supplying the U.S. East Coast. Within days, gas stations from Florida to Virginia began running dry, and panicked motorists lined up at the pumps. In parts of the Southeast, 30% of gas stations were without gasoline. People began hoarding fuel, driving prices to their highest level in six years. One driver in South Carolina canceled weekend plans to conserve gas, noting friends were doing the same. This ransomware-induced fuel outage wasn’t just a technical incident, it disrupted everyday life, causing anxiety and economic loss for families and businesses. The U.S. government even urged the public not to hoard fuel and declared states of emergency to ease transport rules. A U.S. senator remarked that the pipeline hack “is potentially the most substantial and damaging attack on U.S. critical infrastructure ever”, underlining the critical nature of energy OT for society (CISA 2023; U.S. Senate 2021).

It disrupted everyday life, causing anxiety and economic loss for families and businesses.

Electric power grids are equally vulnerable, with failures that carry serious consequences. So far, North America has been spared a large-scale electrical blackout caused by a cyberattack, but smaller incidents hint at the possibilities. In 2019, a ransomware attack on City Power in Johannesburg, South Africa’s largest city, left some residents without electricity after malware encrypted the utility’s databases, applications, and network. Prepaid customers could not buy power credits, effectively plunging homes into darkness until systems were restored. Imagine such an outage during a Canadian winter: families without heating; traffic lights and transit stalled; hospitals relying on generators to keep patients alive.

Hostile hackers have already demonstrated their ability to cause blackouts. During Ukraine’s conflict with Russia,

cyberattacks on the power grid caused widespread outages affecting hundreds of thousands of people in 2015 and 2016. Those were deliberate acts of sabotage, not ransomware for profit, but they prove the point: a successful cyber hit on electrical OT can switch off the lights and life as we know it. For communities, whether in a big city or a rural town, a prolonged power failure isn't just an inconvenience, it's a public safety emergency. Food spoils without refrigeration, people reliant on electric medical devices face danger, heating and cooling systems fail, and emergency services are strained by surges in calls.

It's not only electricity generation that's at risk; distribution of other energy resources is also vulnerable. The Colonial Pipeline incident showed how dependent modern transportation and commerce are on fuel distribution. And just as fuel distribution is critical to transportation and commerce, food production systems are equally vulnerable.

The company ultimately paid an **\$11 million** ransom to resume operations.

In 2021, a cyberattack on JBS, one of the world's largest meat processors, forced slaughterhouses and food production lines across the U.S., Canada, and Australia to shut down. Because JBS supplied roughly a quarter of North America's beef, the incident raised alarms about disruptions to the food supply chain. The company ultimately paid an \$11 million ransom to resume operations, underscoring the extreme pressure to restore critical production and prevent supermarket shortages or price spikes. When the flow of essential goods like electricity, fuel, or food is impeded by an OT failure, people's basic needs are disrupted and economic security is threatened.

Water Systems Under Attack: Poison in the Well

In 2021, a cyberattack on a small Florida water plant in Oldsmar exposed just how quickly an OT breach can become a public health crisis. An intruder breached the plant's control system and remotely adjusted the chemical settings, raising sodium hydroxide (lye) levels in the drinking water from the usual 100 parts per million (ppm) to an alarming 11,100 ppm—a concentration that could have been deadly. Lye is used in trace amounts to control acidity, but at that level it can cause severe chemical burns or poisoning.

Fortunately, a plant operator saw the mouse pointer moving on his screen and reversed the changes in real time before alerting the authorities. Multiple fail-safes and the time it takes water to travel through the system meant residents were never exposed. However, officials didn't mince words: Pinellas County's sheriff called it an "awful intrusion" that could have sickened or killed many people had it gone undetected (Axelbank 2023; Vasquez 2023).

Water infrastructure may not grab headlines like power grids, but it is just as critical. Imagine a similar attack forcing a water utility to shut down or distribute unsafe water: families could lose access to drinking water, sanitation could fail, and contaminated water could sicken anyone who drinks it. In recent years, other cyberattacks on water utilities have occurred, though with less dramatic consequences. In 2022, for example, a major UK provider, South Staffordshire Water, was hit by a ransomware group. While the utility kept water flowing, the attackers claimed to have breached systems controlling water treatment. These attacks may not cause immediate harm, but the resulting anxiety and precautionary measures like boil-water advisories or bottled water runs, affect entire communities. People expect clean, safe water as a given; an OT failure removes that certainty and threatens one of our most basic necessities.

Transportation and Other Critical Sectors: Gridlock and Chaos

OT failures aren't limited to utilities; transportation systems and industrial operations have also been knocked offline, stranding passengers in the process. In 2022, Denmark experienced a nationwide rail disruption when a ransomware attack on a third-party IT provider cascaded into the rail network. The state railway, DSB, halted all trains for several hours after the infected vendor, responsible for train-operating software, shut down its servers to contain the attack. Train operators suddenly couldn't access the

digital system that guides their routes, bringing every train to a standstill. Thousands of passengers were stuck until service was restored, illustrating how a cyber incident can instantly jam a country's transportation arteries. Now picture a similar outage during a Canadian winter rush hour: passengers stranded on freezing platforms, economic activity stalled, and emergency plans activated to manage crowds. In another case, in 2021, hackers took over the regional rail control system radio frequency in Poland and transmitted unauthorized stop commands, causing trains to emergency-brake. Fortunately, no one was hurt, but the incident demonstrated the potential for havoc. When OT transportation fails, the consequences can be catastrophic, from rail collisions to grounded medevac helicopters.

Even road traffic management relies on OT, and that makes it a target. Researchers have long warned that hacked traffic systems could trigger accidents or gridlock. Real-world cases have already occurred: in 2020, a ransomware attack on a Florida municipality disabled automated traffic-light controls, forcing intersections to be controlled manually. Drivers faced congestion and slower emergency response times until systems were restored. While not catastrophic, it showed how easily essential city services can fail, disrupting daily life and even endangering the public.

Beyond transportation, other sectors such as manufacturing and agriculture have also seen OT disruptions with real-world consequences. During the 2021 harvest season, a ransomware attack hit NEW Cooperative, a grain co-op in Iowa. Systems had to be taken offline, forcing staff to revert to manual processes for managing grain and feed distribution. The co-op supplies feed to millions of chickens and hogs, so a prolonged outage raised alarms about animal welfare and impacts on the food supply. One employee described it as the “worst possible time” for a cyberattack, as it coincided with peak crop deliveries and brought digital scale systems and feeding schedules to a halt (Block 2021).

This incident, along with a parallel attack on a U.S. corn mill the same year, highlighted how cyberattacks on agricultural OT can jeopardize food production, potentially leading to shortages or higher prices. Similarly, attacks on OT in critical manufacturing facilities, such as chemical plants or refineries, can threaten public safety. A failure of control systems could lead to spills or explosions, endangering nearby communities.

While major disasters have been avoided, there have been near-misses. In 2017, the NotPetya malware attack crippled pharmaceutical and shipping companies, forcing Maersk's ports offline and halting global deliveries. Workers

suddenly found terminals and cranes unusable, a scenario that, under different circumstances, could have stranded hazardous goods.

These cases show how OT failures ripple through the supply chains, affecting workers, consumers, and public safety.

Public Safety, Not Just IT: Recognizing the Stakes

From operation rooms to living rooms, the stories above make one thing clear: OT security is a public safety issue. Cyber defense can no longer be treated as merely an IT problem. Ransomware and other attacks are literally shutting off the lights and canceling medical procedures. As Brandon Wales, acting director of the U.S. Cybersecurity and Infrastructure Security Agency, warned after the Colonial Pipeline incident, “Cyber attacks on our nation's infrastructure are growing more sophisticated, frequent and aggressive” (CISA 2021). Governments are starting to respond. In Canada, officials have proposed legislation Bill C-8 to strengthen cyber safeguards for critical systems like finance, energy, and transportation. Experts note, however, that healthcare wasn't initially included, a gap exposed by recent hospital attacks. Many are calling for national security standards for hospitals and for healthcare to be treated as critical infrastructure, on par with power plants.

The mindset is slowly shifting: Securing OT is about protecting lives, not just data.

The mindset is slowly shifting: securing OT is about protecting lives, not just data. Practically, this means investing in stronger defenses and emergency response plans for hospitals, utilities, and industry. It means training staff, from nurses to engineers, to recognize cyber threats, and building resilient systems that fail safely. Honest public

communication is also critical, Newfoundland’s 2021 health crisis showed that keeping silent about a breach can erode public trust. Moving forward, transparency, preparedness, and coordination among operators, government, and cybersecurity experts are essential to keep critical services running.

In an interconnected world, a single malicious email or unpatched server can cascade into cancelled surgeries, darkened city blocks, or contaminated water. The human impact of OT failures, as seen in the last few years, is visceral and indisputable. A ransomware-induced power outage isn’t an IT failure—it’s grandparents trapped in elevators and families shivering in cold homes. A hacked hospital network isn’t a privacy issue—it’s cancer patients missing lifesaving treatment and ERs diverting ambulances. Behind the statistics of “downtime” and “data breaches,” are real people who pay the price when OT fails.

The silver lining is growing awareness and action: stronger regulations, better information sharing, and more robust contingency plans. The task now is to accelerate these efforts before the next crisis tests our resilience. Keeping the lights on, water clean, trains running, and hospitals open is a collective responsibility, one that demands the same gravity and investment as protecting human life.®

See [end notes](#) for this article’s references.

[François Guay](#) is the visionary founder of Canada’s largest cybersecurity network, the Canadian Cybersecurity Network (CCN), which unites over 44,000 members from diverse sectors, including individuals, businesses, universities, professional associations, diversity groups, and government agencies, representing nearly 1,000,000 people across the country. Under François’s leadership, CCN has become a cornerstone in fostering collaboration, innovation, and security in Canada’s rapidly evolving cybersecurity ecosystem.



Stay connected

SPONSOR OUR 2026 REPORTS

- State of Cybersecurity (Jan)
- Agentic AI & Cyber (Apr)
- National Defense & Cyber (Sept)



Stronger Together: Securing Critical Infrastructure with IT/OT Convergence

by [Ashif Samnani](#) and [Burt Kim](#), Presented by MOBIA Technology Innovations

Introduction: IT/OT convergence is a strategic imperative

The convergence of Information Technology (IT) and Operational Technology (OT) is transforming the operational landscape for organizations around the globe, particularly in critical infrastructure sectors such as oil and gas, power, water, and manufacturing.

Traditionally, IT and OT have operated in silos. IT focused on data management, cybersecurity, and other shared services. Meanwhile, OT managed industrial control systems, as well as field processes and operations. This made sense when IT and OT systems rarely intersected.

Digital acceleration has changed that landscape. Today's operational technology is increasingly connected to

corporate networks, creating new dependencies, risks, and vulnerabilities. At the same time, cyberthreats have become more sophisticated, targeting IT and OT environments. In response, regulators have placed additional pressure on organizations to establish integrated security that spans both teams.

This new reality calls for IT and OT teams to collaborate in new ways. Working together, they must establish a shared vision, common terminology, and clear context (i.e. roles, governance, and framework) to protect critical infrastructure, control costs, and minimize operational disruptions.

The solution isn't one-size-fits all. Some organizations may pursue convergence, sharing people, processes and technology resources. Others will opt for collaboration, working cooperatively while preserving the distinct cultures of both

teams. The path an organization chooses will depend on its unique needs, size, team dynamics, and strategic objectives. As we explore the business case, unique challenges in the Canadian context, and best practices of IT/OT convergence, we'll use "collaboration" and "convergence" interchangeably in this article to encompass both approaches.

The business case for IT/OT convergence

Organizations around the world are beginning to recognize the strategic importance of unifying IT and OT objectives for several important reasons. Cost reduction is a top priority, especially for asset-intensive industries like manufacturing and oil and gas—where massive capital investments take a bite out of cybersecurity budgets. By leveraging existing IT expertise, these organizations can secure OT environments more efficiently, optimizing costs while enhancing overall protection.

Beyond financial considerations, regulatory pressures are forcing organizations to revisit their approach to IT and OT. Standards like [CSA Z246.1](#), [NIST 800-82](#), [IEC 62443](#), and [NERC-CIP](#) prescribe alignment between IT and OT policies and procedures, making convergence mandatory for compliance.

Finally, IT and OT convergence drives operational efficiency. Integrated asset management and real-time data analytics streamline processes and improve decision-making. For instance, a growing number of utilities and infrastructure operators are adopting unified platforms to manage assets, requiring IT and OT teams to work cooperatively to ensure seamless integration and reduce fragmented systems.

Unique challenges of convergence in the Canadian context

Despite the clear benefits, organizations face a cascade of challenges in achieving effective collaboration. Fragmented systems, for example, are a common roadblock that arises when IT and OT teams implement separate solutions that can't be integrated. This creates inefficiencies and leaves security gaps.

These challenges reflect deeper organizational issues. While IT focuses on confidentiality, integrity, and availability (CIA), OT prioritizes safety, reliability, and availability. Culture clashes, competing priorities, and poor governance alignment between these departments create an environment where siloed communication and misaligned objectives are common.

Beyond these universal struggles, Canadian organizations face additional obstacles. Canada's vast geography leaves many remote regions without fiber-to-the-door connectivity, forcing field sites to grapple with limited bandwidth that hinders real-time collaboration.

IT/OT collaboration best practices for Canadian organizations

For organizations ready to unlock the full potential of IT/OT convergence, a set of best practices can address universal challenges and the unique obstacles posed by Canada's geography.

1. ESTABLISHING INTEGRATED OR CROSS-FUNCTIONAL TEAMS

Cross-functional teams that blend IT and OT expertise foster collaboration and support shared security objectives. The key to creating these teams is in inviting those who are genuinely enthusiastic about convergence and security.

2. DEFINING COMMON OBJECTIVES THAT ARE ALIGNED WITH BUSINESS PRIORITIES

With a single set of objectives that are aligned with business goals, both teams can work toward shared outcomes, such as improving system reliability or implementing innovative technologies.

3. CLEAR AND AVAILABLE COMMUNICATION CHANNELS

Regular meetings and knowledge-sharing sessions facilitate mutual understanding and collaboration. Equally important is establishing reliable communication channels that overcome geographical and connectivity limitations.

4. TRAINING AND DEVELOPMENT PROGRAMS

Training and development equip IT and OT professionals with interdisciplinary skills, preparing teams to adapt to evolving trends and industry standards.

5. LEADERSHIP SUPPORT WITH EXECUTIVE SPONSORSHIP

Leadership support for collaboration between IT and OT signals priority. Taking it a step further, executive sponsorship secures the necessary resources and authority that drive convergence initiatives.

Developing an ideal framework for convergence

Following best practices is an important first step to overcoming common obstacles, but the work of embracing collaboration between IT and OT shouldn't end there.

Creating a common framework provides a structured and sustainable approach that supports technology convergence and strategic alignment across the organization.

A unified risk management system is central to popular security standards and frameworks



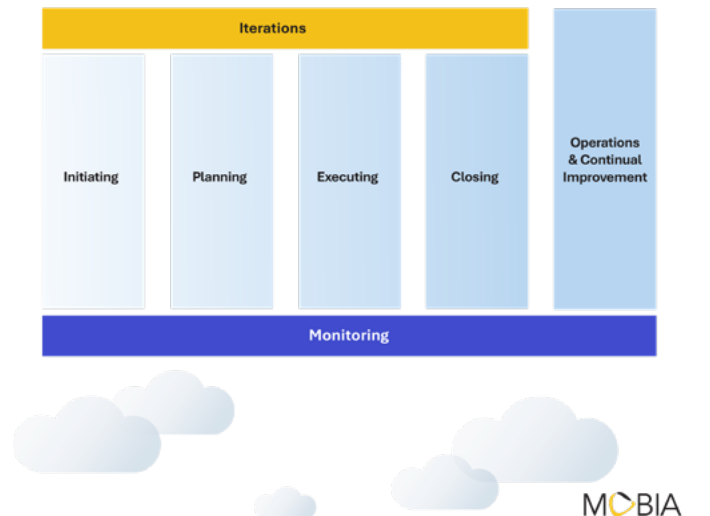
While the ideal framework should be tailored to the unique needs of the organization, standards and frameworks such as ISO/IEC 27001, ISO 31000, and NIST Cybersecurity Framework offer a solid foundation. Risk management is central to these networks, allowing organizations to address threats and vulnerabilities comprehensively and effectively. Starting with one of these frameworks is particularly relevant for organizations operating in regulated industries, where compliance and risk management are paramount.

Furthermore, a tailored framework should include mechanisms for continuous improvement. This might look like regular reviews of collaboration efforts with a focus on applying lessons learned to future initiatives.

A structured lifecycle for implementing IT/OT convergence

With a solid framework in place, organizations need a systematic approach to implement their collaboration initiatives. We recommend a structured lifecycle that moves teams through five iterative phases: initiating, planning, executing, closing, and operations and continuous improvement.

Implementation lifecycle for IT / OT collaboration



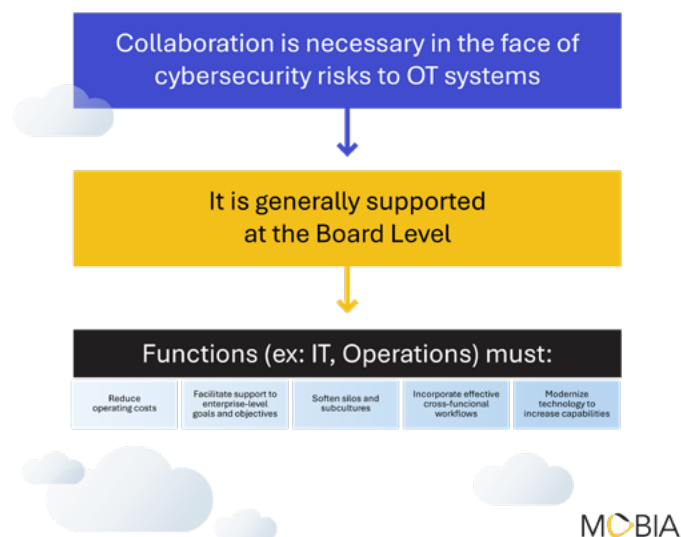
To be successful, organizations must shift and layer their focus as they move through each phase of implementation. In the initiation and planning phases, they focus on engaging stakeholders to get buy-in and clarify expectations. During execution, IT and OT teams participate equally and communicate openly. In the closing phase, teams assess outcomes and identify areas for improvement. Finally, continuous monitoring is practiced throughout the lifecycle to identify risks and opportunities over time. As they work through these phases, successful teams will maintain a unified vision that aligns stakeholders with strategic objectives.

Observations and success factors for IT/OT convergence initiatives

In addition to best practices, frameworks, and structured implementation, a look at case studies and industry initiatives offers valuable insight into the practical side of IT/OT convergence.

As this transformation takes shape across our clients' organizations and others, we have identified common themes and success factors:

Success factors and common drivers for IT / OT collaboration



COMMON THEMES

Cost reduction, cybersecurity, regulatory compliance, and operational efficiency are key drivers for collaboration across organizations with IT and OT environments. However, the obstacles and remediation strategies that prove successful vary depending on the organization's maturity, culture, and structure.

SUCCESS FACTORS

When organizations see convergence as an enabler and not just a methodology, they are better equipped to unify risk management and achieve strategic alignment between IT and OT. This supports them in reducing risks and enhancing resilience.

Investing in cross-training, joint projects, and integrated teams and governance structures is key to success. These investments position IT and OT teams to navigate the complexities of digital transformation and secure critical operations.

Opinion: Leadership and culture make or break collaboration

From our point of view, the success of IT/OT convergence hinges as much on leadership and culture as it does on technology and process integration. Technical frameworks and best practices provide a necessary foundation, but trust, communication, and shared purpose ultimately determines the effectiveness of collaboration.

Leadership support, clear communication, and a culture of continuous improvement are critical to sustaining collaboration and achieving long-term success. Executive sponsorship is more than a best practice when it comes to transformations of this scale. It signals the importance of convergence to the entire organization and provides the resources needed to drive meaningful change.

Conclusion: The future of IT/OT convergence collaboration in Canada

Canadian organizations face more obstacles in facilitating IT/OT collaboration than their counterparts around the world, but we also have a unique opportunity to lead by example. Our diverse and resilient industries, ranging from oil and gas to manufacturing, can serve as testbeds for innovative approaches to digital transformation. By investing in people, processes, culture, and technology, we can build a future where IT and OT work together seamlessly to drive operational excellence, cybersecurity, and business resilience. The journey is not without challenges, but with the right mindset and commitment, the rewards are substantial. ☺

Ashif Samnani is a distinguished cybersecurity leader with extensive experience in operations, risk management, and technology security. At MOBIA Technology Innovations, he serves as Cyber Security Principal and National Practice Leader, where he drives strategic initiatives, leads managed and professional security services, and contributes to thought leadership and customer solution.

Burt Kim is an accomplished cyber security professional and an expert in governance, risk, and compliance. In his role at SimpliGRC, he provides valuable insights into identifying risks and supporting organizations with effective risk management strategies. Burt's work helps organizations implement structured and measurable approaches to security and compliance.



Safeguard your organization's critical environments

At MOBIA, we design solutions and lead initiatives to protect your critical operations from evolving threats.



Strengthen defences across IT and OT networks



Comply with evolving industry regulations



Minimize operational disruptions



Secure your critical operations today.

MOBIA



Why Integrate IT and OT Security?

by [Rob Labbé](#)

Traditionally, even in companies where operational technology (OT) drives most of the revenue and carries the bulk of the risk, cybersecurity teams remain focused solely on IT networks, leaving OT environments out of scope. Once upon a time, this approach made sense. In the early days, OT networks relied on arcane, particular and proprietary networks and technology. Today, that has evolved.

Current OT networks rely on standard IT technology, this includes Windows and Linux, IP networks, virtualization technology and, increasingly, the cloud infrastructure as core elements. With the commoditization of OT, it should

come as no surprise that cyber attacks originating from the IT environments are becoming increasingly common across critical infrastructure and other OT domains.

This shift creates significant strategic and tactical benefits in extending IT security capabilities to OT networks, which requires breaking apart any silos that may exist.

These include:

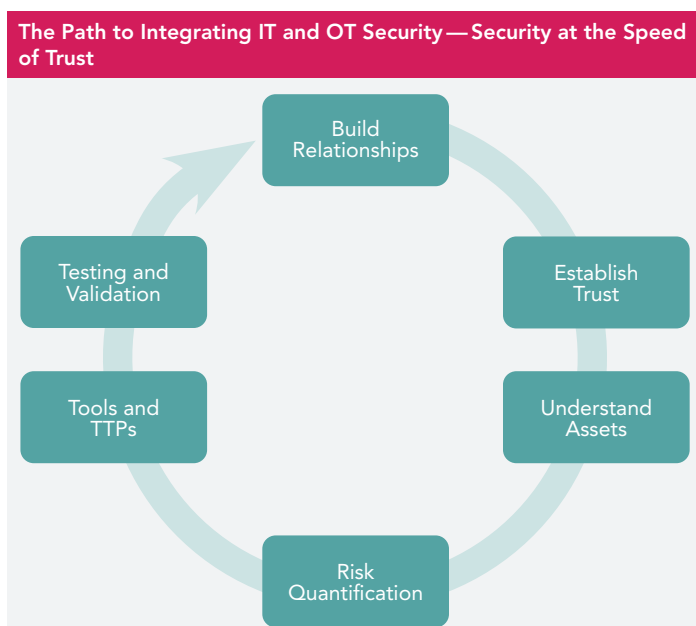
Streamlining of detection and response — The vast majority (well over 90%) of attacks that end up impacting OT start in IT land, be it through a phishing email or other

means. The integration of IT and OT security allows an attack to be tracked across both domains. Unifying detection and response across those domains will only serve to shorten the time to detect, respond and remediate an attack, reducing the overall impact to the business.

Make best use of limited human resources — Integration of IT and OT security will allow you to optimize your security team. It is challenging enough to recruit and retain skilled security teams in major cities; this problem compounds significantly in remote rural areas where mining operations tend to be. By extending your IT teams into OT, you provide an avenue for growth, continued learning, and sharper focus on the organization's key risks; which helps you retain the security talent you already have.

Optimize investment in security tools — Integration in IT and OT security allows you to extend your investment across both environments. This not only creates significant efficiencies over using separate toolsets for security, these security solutions can be used to address operational challenges within the OT environment.

Simplified, centralized risk management — Risk management in OT is always challenging; however, the vast majority of mines and plants have very mature risk management programs in place. With the integration of security into OT, you can begin to show and integrate OT security risks into the existing plant and enterprise risk management system. This centralization of risk (or at least the communication of risk in the same terms) can only lead to a better understanding of cyber risks across the company, leading to improved capital allocation decisions.



Integrating IT and OT security is not a simple task. One of the things that makes it more challenging is the tendency for most security practitioners to approach the issue as a technical challenge. However, OT security is, in my opinion, one of the most human of all cybersecurity domains. Even with strong senior executive sponsorship, many OT security integration projects have failed due to this misaligned approach.

Building trust is essential to reducing safety, environmental and other acute risks inherent in most industrial environments. If you approach IT/OT integration otherwise, you are setting yourself up for failure.

Step 1 — Building Relationships and Personal Trust

Before you can begin to influence, recommend, or discuss security at site, let alone dictate security, you need to earn your right to be present at the table. That starts with building strong personal relationships, which are critical to your ability to build professional trust. This may take considerable time, particularly if the site is in another region, with language and cultural differences to bridge.

OT security is a ministry of presence. The first step is showing up and not just for an hour or a day, but being present for extended periods. Your goals during this time have nothing to do (directly) with security, but rather:

- **Learning the process:** Understand the process from beginning to end. For example: Where are required inputs (raw materials, fuel, parts) from? How does the finished product get to market? Are there any seasonal pressures on production? Where are the bottlenecks? Where are the largest safety and environmental risks?
- **Getting to know the people:** Get to know all the key people at site, not just the general manager and senior leaders. Who are the key influencers? Who is the site process control savant? What are people most proud of? What keeps them up at night? Buy coffee, lunches, and drinks — and listen.

I can't overstate the importance of this step. It will take as long as it takes. In dangerous and high-risk environments, people rely on people, especially those they know and trust.

Step 2 — Establish Trust in your and your Team's Abilities and Approach

Once you have built the necessary relationships and you have earned the right to have a seat at the table, you can now start to talk about cybersecurity. This is the time when

you can identify some “quick-win” security projects. You will no doubt see all sorts of things that are not “right”; security professionals often approach a problem knowing the “right” way to do something. However, in OT, the “right” way is often not the correct approach. Some examples of where you might want to initially tread lightly:

- **Patch management:** In IT, we are used to being able to apply patches very frequently, often monthly or faster. In OT, because of the focus on reliability, stability, and safety, you’ll find your windows to patch being much less frequent, perhaps quarterly or even annually, and subject to stricter testing requirements. Assume this to be the case, and work out your compensating controls.
- **Legacy systems:** We have largely rooted out legacy OSs and Systems in the IT world. However, OT equipment often has a lifespan of 20 years. Because of this you will sometimes find Windows XP (embedded and full OS) or even older OSs in OT. Before you speak about the dangers of legacy OS and push management to replace, take the time to learn why that OS is still there, why it has not been replaced before now. Once you learn that, you will probably discover a more pragmatic approach is needed.

The best candidates for initial security projects are not security projects at all, rather they are site-driven projects aimed at improving stability, reliability, availability and safety, projects that also have happy security side effects. If you have done a good job learning and building relationships in the first phase, you should already have a solid list of these opportunities.

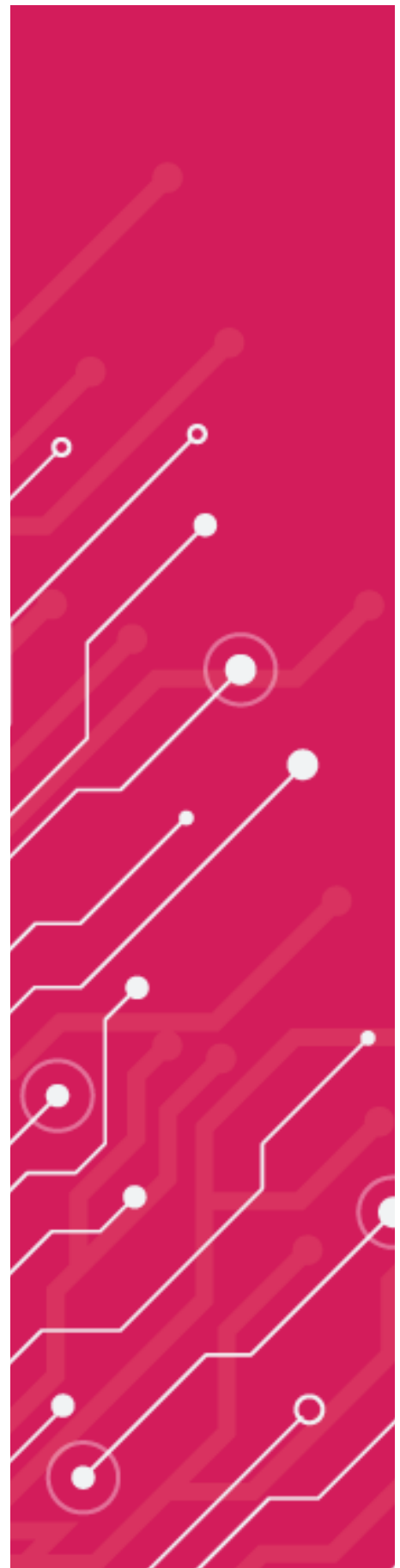
Step 3 — Cover your Assets

Once you have had some initial success and demonstrated your understanding of, and focus on the site’s operational needs, you are ready to build and deploy your security program. The next four steps focus on that program.

Effective asset management is important to any cybersecurity program. This is even more critical in OT environments. Take the time to build an effective asset inventory. In IT environments, you will often find this in a Configuration Management Database (CMDB) or similar systems. In OT, you will often find asset lists in a variety of places – maintenance systems, Excel files, SharePoint lists, somebody’s whiteboard, etc. Don’t expect your source to be the master; rather, work with the site on an effective process to get the information from the system of recording into a place you can work from.

You will also find these lists to be incomplete. Take a few site visits and look for assets. Some methods of looking for assets:

- **War walking/war driving:** Look for unexpected or unusual wireless networks set up at a departmental level or by vendors and service providers at site.
- **Use passive network monitoring:** Look for new IP addresses/MAC addresses popping up on the network and chase those down to their asset. There are a number of tools designed to do this passively in OT networks off a SPAN port; however, with good logs you can do this yourself as well. (Note: Never use an active scanner in OT environments. Many older PLCs and other OT devices in layer 0/1 cannot handle the unexpected network input and may crash.)



- **Don't forget SHODAN:** It is not uncommon for vendors to supply equipment with SIM card slots, connected to the LTE network for management and monitoring. Sometimes these connections supplement your industrial wireless network, in other cases they replace your own industrial network entirely. Shodan still remains one of the best places to find these devices.

Step 4 — Quantify Risk

Before you can begin any security remediation project, or even start deploying a detection and response capability, you must understand and communicate risk.

This step is critical to continuing to build and/or maintain the trust of the site's leadership. It is important to remember that one of the central superpowers of a site general manager is the complete immunity to fear, uncertainty and doubt (FUD). These people get told every day about how the sky is falling and how the plant will come to a stop if they don't invest in x, how the union will strike if they don't do y. Communicating vaguely, and the use of "high" and "critical" (risks) will accomplish nothing for your program or your reputation.

Select a model like FAIR to assist you in getting risk quantified into an accurate number (\$) that all businesses can relate to. Make sure you involve the business in all the inputs to your model, so that when the general manager asks about the conclusions during a site leadership meeting, all his/her senior staff can say they provided the input numbers.

Use that risk framework to justify all your cybersecurity projects, be they remediation/improvement projects or even the extension of your team's detect and response function into the OT environment (our next step).

Step 5 — Extend your Prevent/Detect/Respond TTPs into OT

It is only once you have built the necessary relationships and trust, gained sufficient understanding of the process, technical environment, and risk profile that you can really start to extend the day-to-day security function into the site.

RUNBOOKS/PLAYBOOKS

Start with adapting your IR runbooks and playbooks for OT. Some of the things to consider include:

- **Who are the process experts** at each site? How will you contact them in case of an incident? Who are their back-ups?

- **What is the process to contain a machine?** Most playbooks for infected machines involve some sort of network containment. Often in IT networks, this is fairly low risk; however, this can be a very high risk in OT environments. The containment of a system could eliminate a critical production or safety system.
- **What are the optimal forensics processes?** Most IT systems run with sufficient headroom to allow for active live forensics activities. This cannot be assumed to be the case in OT. Running forensics on live systems may cause instability and unpredictable behavioural impacts — both undesired in OT environments.
- **How do you respond to the worst case?** In the worst case, if safe production cannot be assured, who has the authority to approve a site shut down? What information will they need to make that decision? What situations and circumstances would lead to that action?

LOG DATA

Critical to detection and response processes are logs. The collection of logs in OT can be much more challenging than in IT environments, as many of the system components do not generate log files. However, working to your advantage is the clear text, full trust nature of most OT network traffic. Good network logs can give great visibility into what is happening, particularly in zones 0 and 1.

Getting those logs from OT may be tricky. There may not be switch capacity for SPAN ports, there may not be dark fibre available to run that traffic to your systems; there may even be a general resistance to "touching" the OT network equipment. Again, this is where your relationships can help.

Many engineering teams for control systems struggle with solving intermittent issues in the system and lack the tools to allow them to look at large volumes of network data to find anomalies. The good news, this is where a lot of OT-specific and even general IT security tools shine. Offer the industrial networking and control systems teams access to your anomaly detection (or other) toolsets, give them dashboards that help them find the operational anomalies in the network traffic. Give them that ability and they will move heaven and earth to get that network traffic data to you.

TOOLS

Once you have sorted out log data and your processes, you can select tools that will support those processes and consume that data. Why did we leave tools to last? There is no point in buying expensive tools without well-defined processes or quality data to support them. When looking

at OT environments there are two major categories of tools you'll be looking to purchase initially: Endpoint and Network.

Endpoint

When looking for endpoint solutions, there are a few workable options to choose from. This is an area where there are huge benefits to having a consistent platform across IT and OT, and the natural desire will be to pull the EDR solution you have in IT into OT. This is a good approach if your solution meets the key requirements for an OT EDR solution:

- **On-premise controller options:** All modern EDR solutions require access to a central controller. Most of the time, this is designed to be cloud-based, a perfect solution for most in IT — particularly in this era of hybrid and remote work. To be effective in OT, the solution will need to offer either an on-premise option or some sort of proxy solution that can be deployed at an appropriate location, such as the OT DMZ, to enable communication with OT endpoints.
- **Feature control:** As you deploy in OT, there will be some features, particularly those in the prevent and respond categories, that will be high risk. You will want to disable features that perform intensive forensics or process manipulation, such as automatic containment or process blocking, to allow a smoother initial deployment in a 'detect-only' mode. Then come in after extensive testing to start slipping in those features one at a time, in a highly tuned manner.
- **Transparency:** As you deploy the endpoint solution, you are going to need to deploy to highly safety-sensitive areas. There is a good chance deployment into these areas will

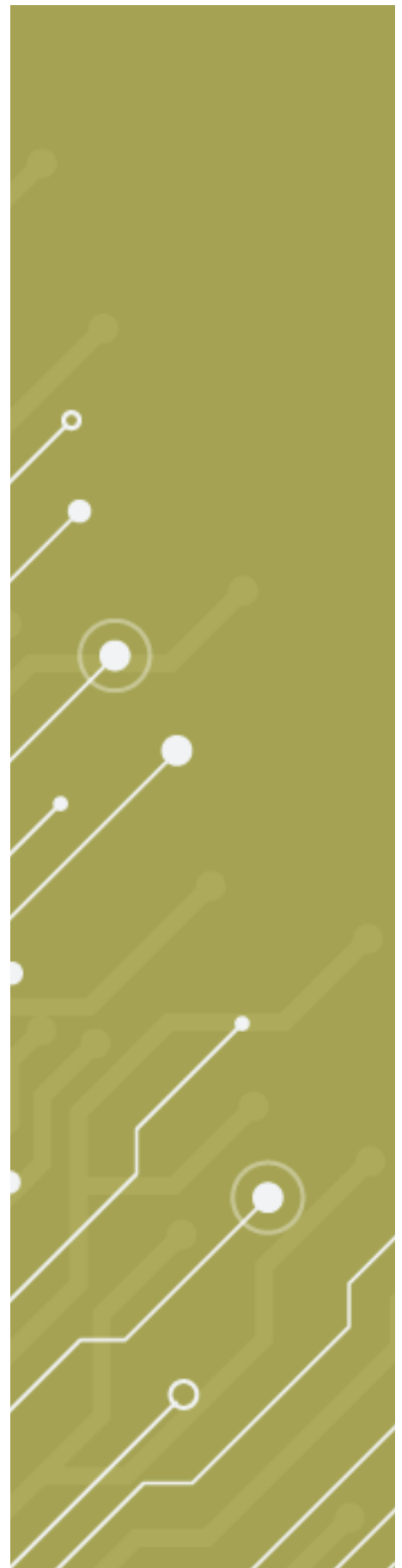
require engineering sign off. You will struggle to get your engineer of record to sign off on a black box. You need a vendor willing to disclose enough of how it works, how the solution is tuned, etc. to get that engineering sign off.

- **Release control:** EDR agents and solutions need to get updated and often. However, particularly in areas that need engineering sign off, you may need to have an alternate release schedule to allow for additional testing of the new agent. Therefore, you need an EDR solution that will allow for agents to be in assorted release states, from current in IT environments to as much as a year old in some OT environments. In OT, tools like SCCM may not be available, which means flexible ways to update in different environments will be important.

Network

Network security systems have come a long way in OT. You will probably want to select an OT specific solution to monitor the OT network traffic, with bonus points if the solution can also be helpful in IT. Again, there are multiple options in the space. Some key features to look for on your shopping list include:

- **OT protocol aware:** The solution should be aware of all the OT protocols used at your sites. The ability to deconstruct that OT traffic and identify anomalous behavioural actions is critical.
- **Useful for operations and security:** Not all OT anomalies have security impact. Many are the root cause of operational challenges. A solution that provides the ability to construct non-security use cases, dashboards, and alerts for the site process control teams will have



much more support at site than a solution that is only for security.

- **Asset discovery and management:** Managing assets in OT environments is challenging because traditional IT discovery methods, such as port scanning are ill-advised at best. Instead, passive discovery capabilities in OT network security products can help you identify the assets, the asset type, and even in some cases firmware information.

Regardless of the solution you choose, deploy slowly, conservatively and incrementally. Start by implementing solutions to the lowest-risk environments, using the most passive configuration possible. Then, increase coverage first followed by capability. Remember: a solution deployed across 100% of the environment with only 20% of the features enabled is still far better than no solution at all—and it gives you a solid basis for expanding capability as you mature.

Step 6 — Testing and Validation

Once you get a site deployed, with your defensive TTPs and tooling in place, the final (and often skipped) step is validation. In the validation phase, you bring it all together with site leadership, integrating your processes into the site's emergency processes and testing them through a tabletop exercise.

All mining sites will have a site-based emergency response plan (ERP), covering a wide range of site issues including fires, geotechnical issues, environmental issues, protests, etc. It is important that your incident response plan integrates into that site ERP. This may include a small section for a cyber incident that delegates to the cyber incident response plan, or something more complex. Either way, it does need to be in there.

Once the plan is in place, it is important to test the plan, at site, as a physical tabletop exercise to work through a severe but plausible incident. This tabletop exercise should involve the general manager, senior site leadership, as well as key OT technical leads.

The goals of the exercise include:

- **Validating your incident response plan** at site
- **Providing an opportunity** for site leadership to experience a cyber incident and your cyber incident response plan
- **Ensuring effective integration** into the site emergency response plan, in particular, for any cyber-physical impacts

- **Testing and validating** chain of command and decision-making processes
- **Validating communications** to corporate decision-makers as well as internal and external stakeholders

Be sure to incorporate the lessons learned from that exercise into both the site emergency response plan and the cyber incident response plan. Schedule recurring tabletops (including after significant updates to your security and/or site landscape) to provide an opportunity to refresh and capture key lessons before an incident.

Finally, these steps are presented as a cycle. You never stop building relationships, building trust and optimizing tools and processes. As those relationships get deeper, you will be able to deploy increasingly robust and capable solutions.

Summary

Integrating IT and OT is critical for holistic security and risk management in mining, metals, and any enterprise heavily dependent on OT. But technology alone won't make it happen, it is a people and trust issue.

Take the time to build trust and relationships before attempting significant technical and process changes—be a student of the process and site. You can only advance your technical and security objectives when you have a license to do so. That license cannot be given by senior leadership; it must be earned through trust. ☺

Rob Labbé has worked in various roles in information security for the past 20 years, the last 12 focused on the cybersecurity of the metals and mining industry. Currently, Rob serves as the CEO and CISO-in-Residence of the Global Mining and Metals ISAC.

In 2016, Rob co-founded MM-ISAC, to build a collaborative community in which threat and incident information is shared, best practices are developed, and relationships are built to improve the cyber posture of the mining and metals industry globally. Rob believes that true resilience in the mining industry occurs when smart, business and user-focused security controls combine with cyber and business resilience. It is only through that user and business-focused lens that companies can both be protected and innovate to produce the minerals and materials the world needs.

In addition to his focus on securing the mining industry, Rob is a fierce advocate for mental health among cybersecurity teams. It is possible to have both a resilient and secure environment as well as a resilient and psychologically healthy team, and Rob is committed to helping organizations in mining and beyond achieve that.



Canada Strong: Rising to the Challenge to Secure OT with Zero Trust Connectivity

by Francois J. Driessen, Presented by ADAMnetworks™

TLDR

- **Rising Threats:** OT environments face increasing risks from organized cybercrime, nation-state attacks, insider threats, and supply chain vulnerabilities, exacerbated by IT/OT convergence and IIoT.
 - **Defense Challenges:** Traditional frameworks like IEC 62443, Purdue Model, and NIST CSF are insufficient against sophisticated attacks. While defenders must secure all vectors with no downtime tolerance, attackers need only one vulnerability to exploit.
 - **Common Denominator:** Most attacks involve egress connections to the Universal Threat Ecosystem (UTE) via the internet, enabling phishing, C2, data exfiltration, or malware delivery.
 - **Zero Trust Connectivity (ZTC):** A Canadian-developed solution that enforces a default, deny-all posture, blocking unauthorized connections without endpoint agents, ensuring resilience across OT/IT, IIoT, and cloud environments.
 - **How It Works:** ZTC gateways provide Layer 2 visibility, automatic device inventory, and distributed control across Purdue Levels, neutralizing threats like shadow IT, malware, phishing, and compromised firmware by preventing egress to attackers.
 - **Benefits:** Disrupts attack chains before execution, integrates with SIEM/SOC for enriched threat data, and allows defenders to focus on neutralized threats, enhancing operational security.
- Conclusion:** ZTC is a critical tool for Canadian defenders, offering sovereign capabilities to protect critical infrastructure and OT environments against advanced cyber threats.

Our world is getting dangerously messy

Demands on the effective protection of OT environments has never been greater than it is today. This is only growing. Cybercrime is becoming more organized with RaaS, while internal threat is enhanced by huge payouts of initial access brokers. At the same time, Nation States are posturing for cyber war with the volatile threat of hacktivists right on their heels.

Defense of OT is an asymmetric challenge. Organizations must secure every attack vector while maintaining already strained operational systems, with zero tolerance for downtime. Meanwhile, the attackers need only a single vulnerability to exploit, often operating with minimal constraints and no downtime.

Protecting critical infrastructure or mission critical operations requires an effective security posture across the entire organization, including its technologies, the humans involved, and the supply chain.

Most of these elements would fall under the direct control of the organization's defenders, but in today's reality, some components will always be out of their control. It is the acceptance of this reality that the defender needs to apply defense-in-depth with, expecting that there will be inevitable failures in each layer.

The tools in play

The tri-mix of IEC 62443, the Purdue Model for Control Hierarchy, and NIST CSF provides core value as a framework for a resilient security posture. Yet organizations that have implemented these frameworks and passed rigorous compliance audits continue to fall victim to breaches and

disruption, with no significant sign that mounting risks are decreasing.

The odds remain badly stacked against the defender.

CHALLENGES FROM:

- **Sophisticated ransomware**
- **Supply chain breaches** including compromised device patches
- **Nation-state attacks** involving espionage and OT-specific sabotage
- **Full scale cyber war**
- **Phishing exploits**
- **Insider threats** fuelled by Initial Access Brokers (IAB)
- **Intellectual property theft**
- **Human error or shadow IT** bridging Purdue layers
- **AI-enhanced adversarial tactics** and effective Detection Evasion

On their own, these challenges are more than enough to cause critical failure. Together, they form a composite risk level that dwarfs what defenders were facing just a few decades ago. These threats are exacerbated by converging IT/OT environments, driven by emerging IIoT technologies and the increase of cloud based systems colliding with legacy system integrations. By simple definition, remote access and the air-gap perimeter-based models are in direct collision.

The common denominator:

A clear picture emerges when dissecting OT incident response cases over the last 5 years: Things go wrong even when defenders do most things right. Critical failure in North America today does not generally come from gross negligence, but rather from the imperfect application of the current stack of tools and security structures we rely on. For example, an industrial laser

was bridged to the internet via shadow IT so technicians could troubleshoot remotely, or a firmware patch that contained malware, waiting for a signal from a command-and-control server to trigger disruption.

In the tactics captured by MITRE ATT&CK, there is one common denominator floating to the surface for an overwhelming number of use cases, regardless of the motive for the attack: an egress connection from the victim network is used as a step of the attack chain. This connection can serve various purposes: phishing, reconnaissance, Command & Control (C2), data exfiltration, or accessing the next payload of the attack, such as direct implants of insider threats.

A key deduction: once a device can connect to the open Internet, it can also potentially connect to the infrastructure of the attacker. This could happen directly or through a hop from another device within the isolated segment. For the purpose of this article, we will refer to the Internet as the primary bridge to the Universal Threat Ecosystem (UTE).

Relying on the notion of an air-gap or segment for security may offer a sense of protection. But a single human error, shadow IT workaround, or compromised firmware patch can quickly result in a direct point of access for the attacker. The entire segment or layer can be swept into disruption, extortion, or even destruction.

Enter Zero Trust Connectivity

The good news is that, in many cases, the common denominator of the UTE, accessed via the internet, is a centralized element that the defender can now focus on. Shut down egress to the attacker, and you disrupt the attack. What's even more valuable, is that if you have the capability to



apply this by default, it is possible to disrupt the attack before it can execute. The detection evasion threat becomes irrelevant, since no detection is required in a default deny-all state.

Assume breach: Layer your defense-in-depth structure so that you are not only prepared for failures in the normal state of your security, you actively expect failures as the new norm.

Enter Zero Trust Connectivity (ZTC): A novel Canadian developed technology that has matured over the last 10 years. It is now being rolled out to enterprise, critical infrastructure, and mission critical OT environments. The philosophy involves moving your networks and operational control into whatever state you would be in by the time you would have detected a breach; using intelligent systems to facilitate full operational resilience while operating this hardened state.

To achieve this posture, all connections are disallowed by default unless requested by a verified device and to a specified destination. This is applied at various policy sets appropriate for each operational layer, to allow operational resilience while maintaining a hardened posture against potential UTE exposure.

Implementing Zero Trust in OT and IoT environments introduces additional challenges due to the restriction of applying endpoint agents. For this reason, ZTC was designed to operate out of band and without the need of an endpoint agent. Applying Zero Trust control through the network gateways allows full Layer 2 visibility for automatic device inventory. Without the requirement of an endpoint agent, all devices with potential connectivity can be protected - regardless of device type. This specifically addresses the OT/IT merger, IIoT and cloud native services for emerging technologies such as AI enriched sensors.

A decentralized Muscle-Brain configuration allows for distributed application of multiple ZTC gateways throughout the Purdue Reference Levels, while centralized control allows a single pane of glass for policy assignment. This facilitates multi-site and multi-tenant management that allows for the sharing of policies and configurations between them.

Since every single connection request is visible by the gateway, the default deny-all posture automatically blocks shadow IT that might otherwise bridge Level zones and compromise isolation.

Integration with SIEM and SOC systems provides highly enriched data on potential risks. However, because of the default-deny-all posture, many uncovered threats are already

neutralized by the time they are detected by integrated systems. This allows defenders to have a first-mover advantage over attackers, and exhaust the attacker's resources effectively to either move on to another target or abandon the attack altogether.

Where ZTC fits into the Security Stack

ZTC is enabled by a protective resolver purpose built for ZTC, tightly integrated with a firewall engine that can simultaneously operate securely with or without DNS. Firewall rules are written and destroyed at the order of 10,000 per second, driven by the policy engine. As a general rule of thumb, ZTC nodes are inserted wherever traditional firewalls would have been deployed.

The core application would cover IoT and IT in Level 5, but it should also serve as a protective layer between any external internet connection and the organization's internal network. From there, ZTC nodes are distributed down to lower Levels of IIoT and OT, enabling centralized control over additional physical segments and layers, as well as vastly enriched data feeds to SIEM / SOAR. East-West traffic within Levels is also controlled by segmentation from the ZTC gateway.

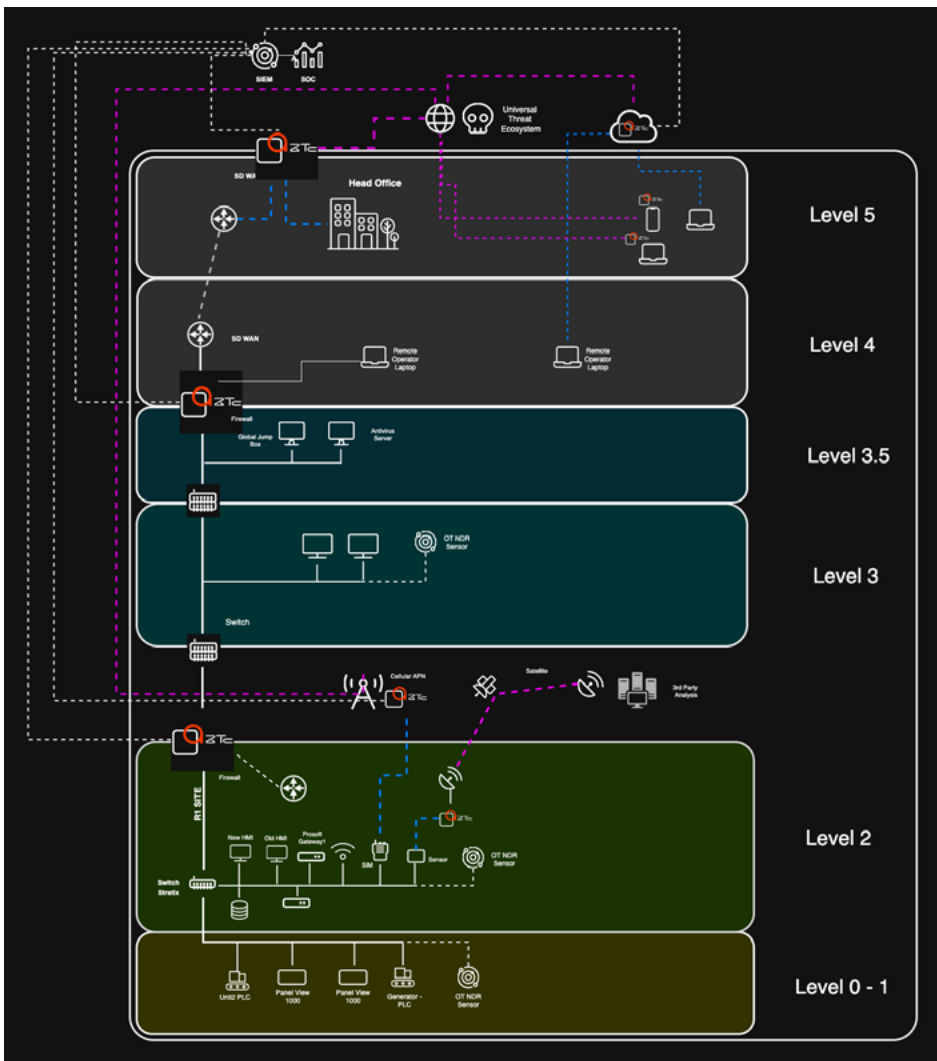
ZTC nodes run in High Availability (HA) pairs to provide resilience. Updates to muscle instances can be rolled back instantly, if required, without taking the secondary node off-line. Firmware changes on OT do not affect the performance of ZTC nodes, as they function independently of agents and are completely device agnostic. Additionally, ZTC nodes can enforce very strict access controls during rolling updates and diagnostics for any OT elements.

Since this closes the door for the attacker egress, any demarcation point where internet connectivity is possible is an ideal place for a ZTC node.

For technologies with direct cellular connectivity, ZTC can be extended by deploying a ZTC within the cellular provider's data centre, enabling a dedicated Access Point Network (APN). For direct satellite connectivity, a dedicated node can be introduced between the modem and the device.

The same is true for roaming or multi homed IT devices, regardless of their network segmentation level. In these cases, additional options include the use of a dedicated VPN to a ZTC node, or embedding the ZTC resolver directly onto the device in the form of an agent.

Detection sensors can be layered within network segments through the ZTC gateway. If indicators of compromise



are detected, the gateway can move affected devices into a quarantine state, should the SOC team choose to take further action beyond the default egress control already applied to all devices.

Test cases

To explore the attack disruption value of ZTC, here are some examples of how ZTC disrupts the attack chain:

SHADOW IT BRIDGES A ZONE GAP

Level 2 ICS: Technicians are required to troubleshoot a defective industrial laser. To facilitate remote diagnostics, an employee disregards security protocols and temporarily connects the laser to the Internet.

This remote access remains open, and an attacker finds a way into the Level 2 segment. Under normal circumstances, the security team would be completely oblivious to the unfolding breach.

>ATTACK DISRUPTED<

The ZTC gateway immediately sees a new device connecting to the network segment and automatically places it in the default quarantine state. No connection is allowed and thus no egress is made available for an attacker to exploit.

With no other choice but to follow security protocol, the employee follows the appropriate channels to have a secured connection established to the remote technician. The security team

assigns a policy that allows connection to the remote technician, and only that connection alone, which is collapsed once the service is complete.

IMPLANT OF MALWARE BY AN INSIDER THREAT

Level 4 Workstation. An insider threat plugs in a flash-drive and runs a malicious application.

The malware attempts to reach the C2 server via a direct IP or FastFlux FQDNs for security circumvention & resilience.

>ATTACK DISRUPTED<

ZTC denies access to all direct IP requests unless they are first resolved via DNS and permitted by AI-driven policy - regardless if the IP is block-listed or not. This connection request is captured by the log and passed on to SIEM.

Since it is a novel attack and the IP does not exist on a block-list yet, threat intelligence takes some time to flag it as malicious. This is inconsequential since the attack is already contained, preventing any follow-up actions or lateral movement. Once SIEM or the SOC intelligence catches up, the workstation can be quarantined and restored with forensics analysis.

The additional value to the defender here is that the SOC is looking at an event that could have caused a breach, and not a breach that has already occurred.

SPEAR PHISHING ATTACK TO DEPLOY RANSOMWARE THROUGH THE ENTERPRISE NETWORK

Level 5 Workstation. An employee receives an email with a malicious attachment that manages to bypass other security controls. This executes a dropper or loader on their corporate workstation. The loader reaches out to newly-minted (or strategically aged) domains that are not yet on any threat intelligence block list.

>ATTACK DISRUPTED<

The default deny-all state of ZTC sees the domain as un-verified since no proper reputation exists. The connection request is denied, preventing any additional payload from reaching the workstation.

The log is passed on by the ZTC gateway in real-time to the SOC, which can respond to the incident that is already contained by the ZTC gateway. Additional automation from the SIEM directs the ZTC Gateway to quarantine the infected workstation, allowing the security team to perform cleanup and forensic analysis.

COMPROMISED FIRMWARE PATCH

Level 2 ICS: A supply chain vulnerability introduces advanced malware through a compromised firmware patch. The malware is designed to bypass traditional firewalls using PLCs as proxies, similar to tactics seen in attacks like Industroyer.

Its activation does not rely on a single specific trigger, this toolkit activates only after its components are successfully deployed within the target environment. Its modular architecture and automated functionality make it user-friendly, allowing even low-skilled threat actors to emulate advanced persistent threat (APT) capabilities.

>ATTACK DISRUPTED<

Communication between the malware kit and the attacker's Command and Control (C2) server is severed by default via the ZTC gateway. Although the malware exists within the OT environment, it remains dormant with no method to connect to the attacker.

Monitoring of ICS traffic and real-time connectivity logs from the ZTC gateway to SIEM surfaces the presence of the malware, appropriate steps can then be taken to roll back the firmware update to a safe version.

Conclusion

There is no question that Zero Trust brings an additional force multiplier for defenders facing advanced threats in OT today. ZTC provides the flexibility and versatility needed across OT, IT, and IIoT, allowing defenders to move the entire organization into a Zero Trust state.

The value of getting an alert in the defender's SIEM or SOC for threats that have already been neutralized, before they were detected, is a value that is hard to overstate. The asymmetric odds against the defender can now be changed with the proper application of ZTC technology.

Canada needs sovereign capabilities. ZTC provides these capabilities, equipping our defenders with the tools needed to protect our industry and critical infrastructure.®

Francois J. Driessen is the COO, CMO and Co-Founder of ADAMnetworks™. Francois' key mission is to have technology serve people, and not the other way around. He leads operations & marketing for the ADAMnetworks team with the primary goal to protect people and the systems they rely on. BaBk(IOW) in Information Design. IMDb 3524652. Co-Founder of EdgeFactor. Founder of FireTrigger Inc. Over 30 international awards ranging from Creative Direction, UX Design, Digital Media & Film.

Research Assistant: [Jed D.S. Sananda](#)



//adamnet.works

reflex AI

adaptive AI

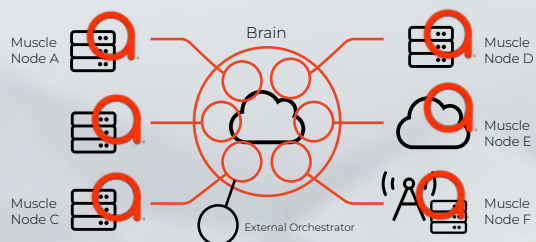
DTS
don't talk to strangers

adam:ONE®

Next Generation **ZTC** EDGE

Proactively deny connections of all potential threats while intelligently remaining connected to all that is good and necessary.

- **Neutralize Ransomware, Zero Days & Evasion Threats** BEFORE detection.
- **Exfiltration of Classified Data & IP theft stopped** BEFORE attacks can execute.
- **Phishing Vector Closed by default.** Effectively mitigate the Human Factor.
- **IoT | IIoT | MIIoT | OT | ICS | CI protected.** No agent required.
- **Sovereign Data Custody.** Decentralized resilience.
- **Resolve Shadow IT.** Automatic Device Quarantine. Full Layer2 Visibility.
- **M-22-09 easily fulfilled** across all devices and environments with minimal disruption.



How adam:ONE® works

At the core, adam:ONE® is a ZTC capable caching resolver that is tightly integrated with a Firewall and operates in a Muscle - Brain hybrid configuration: Gaining the resilience of a distributed deployment and the benefit of centralized control. Out-of-band protection means its protection is applicable to all types of devices including OT, IoT and IT with no endpoint agent required. The Muscle can be applied to a flexible edge on-premise or in-cloud at any point between the endpoint and its connection to the Universal Threat Ecosystem (a.k.a.: the Internet). A cloud controller (Brain) is used for orchestration and controls.

1. Starting in a Default-Deny-All state, by the use of aggregated intelligence merged with AI driven dynamic allowlisting, a dynamic policy is written as a verified device requests access to verified connections.
2. Patented technology called Don't Talk to Strangers (DTS)® denies all IP connections by default, unless authorized by an Enabler, or first requested by DNS and allowed by the a dynamically generated policy.
3. If allowed by policy, it opens a hole to establish the verified connection, and then collapses it as soon as the connection expires.

Allowed connections using DNS are cross-checked by DNSHarmony® aggregation of protective DNS resolvers of your choice. This aggregates threat intelligence in real-time for enhanced performance and creates resilience beyond the standard single resolver set.



The net result: **Zero Trust connectivity for any device requesting connection through adam:ONE®.**
ZT protection invisible to the user.



Best SASE 2024
Best SASE 2025



SASE 2024



SASE Solution
of the Year



Customer Sentiment

Reduce your Attack Surface 7000:1.

contact@adamnet.works

See adam:ONE® in Action
<https://adamnet.works>



All items © 2025: Adam Networks LLC. All trademarks are the property of their respective owners.

Conclusion & Recommendations

Operational technology is no longer behind the scenes, it is the stage on which Canada's safety, prosperity, and resilience are actively shaped. From the power that lights our homes to the hospitals that save lives, and the mines, pipelines, and transportation systems that fuel our economy, OT security is the thread that keeps our country running. As this report has shown, the threats are real, growing, and increasingly sophisticated. We are seeing ransomware that halts surgeries, hostile probing of energy grids, and cascading risks introduced by IT-OT convergence.

But the message is not one of alarm alone, it is also one of opportunity. Canada is not starting from scratch, it has world-class cybersecurity talent, innovative companies, and a collaborative ecosystem built for this challenge.

By **strengthening** resilience, **improving** intelligence sharing, **modernizing** systems, and breaking down barriers between IT and OT teams, we can build a future where critical infrastructure is not only **defended**, but made **stronger**.

The Canadian Cybersecurity Network is committed to leading this national effort. With over 45,000 members and voices from every sector, we will continue to convene, connect, and champion the cybersecurity priorities that matter most. The stakes could not be higher, securing our OT means securing the Canada we want to live in, safe, innovative, and resilient for generations to come.®





stay connected

**SPONSOR OUR
2026 REPORTS**

**State of Cybersecurity (Jan)
Agentic AI & Cyber (April)
National Defense & Cyber (Sept)**

References

Why Critical Infrastructure Must Prioritize Cybersecurity by Enza Alexander

¹ The Canadian Centre for Cyber Security (CCCS) contributed to a [May 2024 fact sheet](#) issued by CISA that highlighted increased foreign interference, along with resources to help defend against these sophisticated attacks.

² Fortinet's [2024 State of Operational Technology and Cybersecurity Report](#) revealed that unintentional insider breaches were involved in 50% of OT-related incidents in 2024; nearly double that of 2023.

³ Ibid at 13.

⁴ See [Reuters, 2024](#).

⁵ See [HIPAA Guide, 2024](#).

⁶ See [Bill C-8](#).

From Guidelines to Guardrails: The Power of Deploying Cybersecurity Standards in Canada's Industrial Sector by Denrich Sananda and Sonia Khan

An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts – [Parliament of Canada](#)

[NIST Cybersecurity Framework](#)

[ISA/IEC 62443 Series of Standards: The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards](#)

[ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements](#)

[Security management for Critical Infrastructure](#)

The Human Impact of OT Failures by François Guay

[Axelbank, Evan. 2023. "Hack of Oldsmar Water Plant Reported Two Years Ago Could Have Been Employee Error." FOX 13 Tampa Bay. April 11, 2023.](#)

[Block, Tom. 2021. "Iowa Grain Co-op Hit by Ransomware Attack." Iowa Farm Bureau. September 27, 2021.](#)

[CISA. 2021. "Statement from CISA Acting Director Wales on Executive Order to Improve the Nation's Cybersecurity and Protect Federal Networks." Cybersecurity and Infrastructure Security Agency. May 13, 2021.](#)

[CISA. 2023. "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years." Cybersecurity and Infrastructure Security Agency. May 7, 2023.](#)

[Cluley, Graham. 2023. "Cancer Treatments Cancelled after Canadian Hospitals Hit by Ransomware Attack."](#)

[Canadian Healthcare Technology. 2023. "5 Hospital CEOs Report on Impact of Ransomware." Canadian Healthcare Technology. November 22, 2023.](#)

[La Grassa, Jennifer. 2023. "CEOs of Ontario Hospitals Hit by Ransomware Attack Break Down Impact on Operations, Patients." CBC News. November 17, 2023.](#)

[O'Neill, Patrick Howell. 2020. "A Patient Has Died After Ransomware Hackers Hit a German Hospital." MIT Technology Review. September 18, 2020.](#)

[Silomon, Jantje. 2020. "The Düsseldorf Cyber Incident." IFSH. September 30, 2020. <https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident>.](#)

[U.S. Senate Committee on Homeland Security and Governmental Affairs. 2021. Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyberattack. Hearing, June 8, 2021.](#)

[Vasquez, Christian. 2023. "Did Someone Really Hack into the Oldsmar, Florida, Water Treatment Plant?" CyberScoop. April 10, 2023.](#)

