Bridging the IT/OT Security Gap

The convergence of information technology (IT) and operational technology (OT) is rapidly changing the industrial landscape due to the increased efficiency and automation it brings. The integration of IT/OT networks allows industries such as energy, manufacturing, water treatment, and transportation to enhance their operations and leverage real-time data to optimize processes. However, this convergence also introduces new security risk, increasing the attack surface of industrial control systems (ICS) and other OT environments. While securing traditional IT systems typically involves confidentiality, integrity, and availability (CIA), OT systems focus more on uptime, safety, and reliability due to their critical nature. As these once-isolated OT environments become increasingly connected with broader IT networks—often through IoT, cloud, and remote access technologies—they inherit a range of cyberrisk factors that they were never designed to withstand.

The result is an expanded attack surface where vulnerabilities in traditional IT systems can serve as entry points into critical OT infrastructure. Compounding the problem is the fact that OT systems often rely on legacy hardware and proprietary protocols that lack modern security features and cannot be easily updated or patched. This convergence introduces not only technical complexity, but also operational and cultural challenges, as cybersecurity priorities and practices differ widely between IT and OT teams. Understanding these differences—and how to bridge them—is essential for protecting industrial systems from increasingly sophisticated cyberthreats.

Understanding IT/OT Convergence

IT/OT convergence refers to merging traditional IT environments that handle business, data, and applications with OT systems associated with industrial processes and physical hardware. Traditionally, these two environments existed separately, with organizations typically air-gapping (i.e., physically isolating computers/networks from external systems) their ICS and other critical infrastructure from the enterprise's IT environment.

The rise of the Internet of Things (IoT) and cloud-based automation has given industries such as water, transportation, and utilities the ability to analyze industrial data in real time for better performance and cost optimization. The trend shows no signs of stopping anytime soon, with a recent IT/OT Convergence Insights report estimating the combined IT/OT market to surpass US$1 trillion by 2030.[1]

However, this means that previously isolated systems are now exposed to the same cyberattacks that traditional IT environments experience. Unfortunately, securing these environments is not as simple as extending the coverage of existing cybersecurity controls to OT systems.

PRANJAL SHARMA

Is a senior software engineer with more than 13 years of experience in cloud computing, distributed systems, artificial intelligence (AI), machine learning (ML), cybersecurity, and zero trust security. He has a diverse background in technology development and sales. Sharma has contributed to multiple Institute of Electrical and Electronics Engineers (IEEE) conferences as an author, publication reviewer, and chair, particularly in the fields of cybersecurity and cloud computing. His expertise spans a wide range of technologies, including advanced network security protocols, scalable cloud solutions, and data privacy frameworks. He is currently focused on implementing zero trust architectures to enhance security in distributed environments, working towards building resilient systems for organizations adapting to modern security challenges. Sharma is also the inventor of a pending patent related to cloud-based security architecture.

FIGURE 1

Comparing Cybersecurity and OT Security

Cybersecurity	OT Security
Prioritizes data confidentiality, integrity, and availability	Prioritizes uptime, reliability, and safety
Regular software updates, patches, and automated security controls	Legacy systems that cannot be easily patched or updated
Employs firewalls, endpoint detection, and threat intelligence for protection	Requires air-gapping, physical security, and real-time process monitoring
Involves business applications, email, cloud storage, and databases	Controls supervisory control and data acquisition (SCADA), ICS, sensors, and industrial machinery
Cyberrisk includes phishing, ransomware, and data breaches	Cyberrisk includes disruptive attacks, sabotage, and physical damage

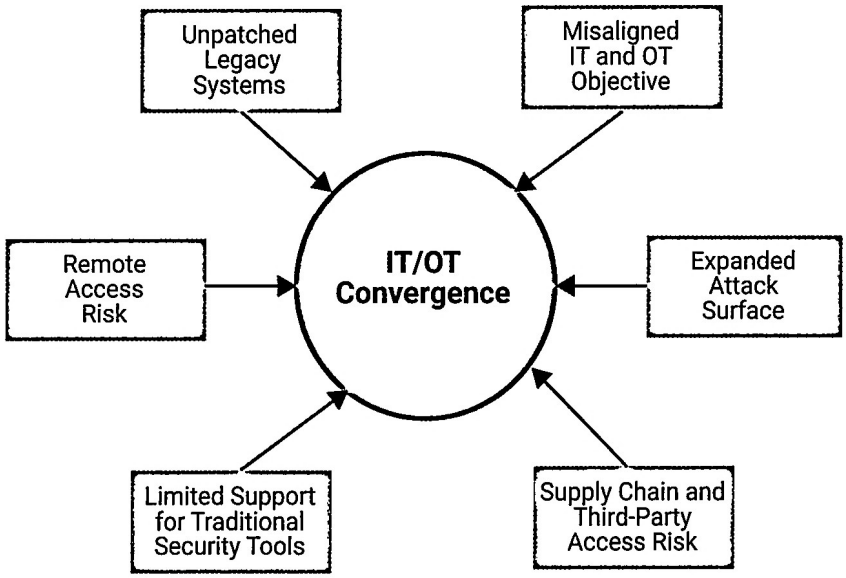
Cybersecurity Challenges of IT/OT Convergence

To understand the unique challenges that arise from IT/OT convergence, there is a need to examine some of the key security differences between traditional systems and OT systems. **Figure 1** shows a comparison of traditional cybersecurity and OT security.

These differences make securing merged IT/OT environments much more complex, as evidenced by the challenges depicted in **figure 2**. Traditional security controls such as endpoint detection, patching, and scanning may not be extendable to OT systems, where downtime can have a catastrophic impact on society and human life.

FIGURE 2

Overview of IT/OT Security Convergence Challenges



Consider the example of ransomware, easily one of the most disruptive threats to modern organizations. While traditional IT environments may suffer from loss of availability and financial loss, the consequences in an OT environment can have crippling effects on society and even public safety. The risk is further amplified by the fact that OT environments typically do not follow the regular patching cadence of traditional IT systems.

In 2021, cybercriminals were able to compromise the network of Colonial Pipeline, the largest pipeline operator in the United States.[2] Despite the OT system network not being impacted by the attack, the decision was made to shut down the pipeline to prevent the attack from spreading, leading to shortages across the country. This incident can be seen as an example of the risk that arises from IT/OT convergence and how attacks on traditional systems can cascade to more critical infrastructure.

There is no shortage of additional challenges that arise from IT/OT convergence.

Expanded Attack Surface

Connecting IT and OT environments means that attackers can potentially exploit vulnerabilities and risk present in IT environments to gain a foothold in OT environments. Removing the air gap (i.e., the physical isolation from the external networks) may provide productivity and efficiency benefits, but it exposes OT systems to cyberrisk that may not have previously been present. Without effective network segmentation, attacks can move laterally between networks until they reach and compromise OT systems.

Limitations of Legacy Systems

Most OT systems run on legacy applications that are not easily patched or remediated due to their mission-critical nature. These systems are often designed to prioritize availability and resilience, not cybersecurity. They can be operational for decades without downtime and often utilize proprietary protocols that do not support modern security mechanisms such as encryption and authentication. Such limitations also mean that attackers or nation-state actors can compromise long-running unpatched systems and take control of OT systems to their advantage.

Lack Of Security Visibility

Cybersecurity teams often do not have the same visibility into OT networks due to their closed nature, making it difficult to detect anomalies or patterns indicating a cyberattack. Additionally, traditional security information and event management (SIEM) and endpoint detection and response (EDR) solutions often do not support OT systems and protocols, making these devices a security blind spot that can be exploited.

Differing Priorities

OT teams are often asked to ensure operational continuity and uptime at all costs. This usually puts them at odds with security policies and controls, leading to potential cultural clashes when these environments are converged. This often-overlooked challenge can stall cybersecurity initiatives if not accounted for.

Supply Chain Risk

Due to their proprietary nature, OT environments often require external vendors to be provided access for maintenance, increasing the risk of potential third-party breaches. The closed nature of OT systems makes it challenging to monitor the work being carried out to ensure that no security risk is introduced. Thus, supply chain attacks become a key risk within IT/OT networks, with attackers compromising a trusted third party and using it to piggyback into a secured OT environment digitally. The SolarWinds incident, in which cybercriminals inserted a malicious payload into the popular monitoring platform and compromised countless organizations, is a key example of this type of attack.[3] This attack also spread to numerous critical infrastructure and OT environments due to their trust in SolarWinds.

The security of OT environments must always be balanced with performance and operational requirements, regardless of whether an organization is dealing with a converged or isolated environment.

Remote Access Risk

One of the key benefits of interconnectivity is the ease with which OT environments can now be monitored and controlled. However, this also means attackers can compromise insecure remote-control software to gain access to such environments. Vulnerabilities such as weak or default passwords, lack of multifactor authentication (MFA), and misconfigured virtual private network (VPN) are weaknesses that can have devastating impacts if exploited successfully. Consider the example of the US state of Florida water treatment attack in 2021, in which attackers compromised a water treatment plant via remote access software.[4] While this attack was thwarted, it shows the real danger in interconnected environments and remote access.

Mitigating the pressing challenges that arise in an interconnected environment requires a multifaceted approach, one that balances risk mitigation without compromising the operational efficiency that systems require.

Best Practices for Securing IT/OT Environments

The security of OT environments must always be balanced with performance and operational requirements, regardless of whether an organization is dealing with a converged or isolated environment. A well-structured security strategy will integrate technical, operational, and governance controls to mitigate threats without disrupting industrial processes.

Applying Network Segmentation and Zero Trust Principles

Converged IT/OT environments mean that the air gap no longer exists, and a cyberattack in IT can potentially move laterally into OT systems unless networks are adequately segmented. Zero trust

LOOKING FOR MORE?

- Learn more about, discuss, and collaborate on cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforum*

Organizations must stay ahead of emerging cybersecurity risk while leveraging new technologies to enhance threat detection, resilience, and operational efficiency.

principles that do not assume any implicit trust and treat all traffic as potentially malicious can greatly help converged environments.

Some best practices for such converged environments are:

- Ensure that separate network zones are present for OT and IT environments with firewalls and intrusion/detection systems on all network boundaries to monitor unauthorized traffic.
- Implement demilitarized zones (DMZs) to control traffic between IT and OT environments.
- Enforce restrictions on east-west traffic within OT environments to prevent malware from moving laterally.
- Adopt least privilege access policies for OT engineers, vendors, and remote operators.
- Enforce MFA for all IT/OT remote access connections.
- Implement role-based access control (RBAC) and privileged access management (PAM) to prevent unauthorized actions.
- Use network access control (NAC) to enforce security policies for all devices connecting to OT networks.

Enforcing strong segmentation and zero trust principles can help organizations reduce the risk of cyberattacks spreading across IT and OT environments.

Adopting Cybersecurity Frameworks

Adopting industry-recognized security frameworks is essential for standardizing IT/OT security practices. There are several frameworks that provide guidelines for risk management, security controls, and compliance in industrial environments.

NIST CSF

The US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is an industry benchmark that provides a structured approach to managing IT/OT integration cybersecurity risk.[5]

Key components include:

1. **Govern**—Establish cybersecurity policies; roles, responsibilities, and oversight for IT/OT systems.
2. **Identify**—Conduct asset inventories for both IT and OT networks.
3. **Protect**—Implement security controls such as firewalls, encryption, and access controls.
4. **Detect**—Deploy SIEM and anomaly detection systems for continuous monitoring.
5. **Respond**—Develop incident response plans for cyberthreats affecting IT/OT.
6. **Recover**—Implement backup strategies and disaster recovery plans for OT continuity.

ISA/IEC 62443 for Industrial Cybersecurity

The International Society of Automation (ISA)/International Electrotechnical Commission (IEC) 62443 is a global standard for securing ICS.[6] It provides guidelines for risk assessment, patch management, and supply chain security. Organizations can certify their OT security posture based on this framework.

By aligning with these frameworks, enterprises can enhance security resilience, meet compliance requirements, and improve threat response capabilities.

Threat Detection and Real-Time Monitoring in OT Networks

One of the biggest challenges in OT security is the lack of visibility into network activity. Many ICS and SCADA systems were not designed with cybersecurity in mind, making the detection of cyberattacks, malware, or unauthorized access difficult.

Some key best practices for IT/OT converged environments are:

- Deploy SIEM tools with OT-specific integrations.
- Leverage OT-specific threat intelligence to receive notifications of any planned attacks against critical infrastructure.
- Implement artificial intelligence (AI)-driven anomaly detection to identify unusual behavior in OT environments.
- Conduct continuous security assessments to identify misconfigurations and vulnerabilities.

Patching and Hardening Legacy OT Systems

Since many OT systems cannot be patched frequently, alternative security measures must

be implemented to mitigate vulnerabilities while maintaining operational uptime. Some key strategies for securing legacy systems are:

- Implement compensating controls such as network segmentation and whitelisting to reduce exposure.
- Use virtual patching via intrusion prevention systems (IPS) to block known exploits.
- Increase the level of monitoring on these systems to compensate for the lack of patching and hardening.
- Restrict internet access for OT systems as much as possible to reduce exposure to external threats.

Securing IT/OT convergence requires a multilayered cybersecurity approach integrating network segmentation, real-time monitoring, secure access controls, and adherence to cybersecurity frameworks. There is also value in exploring future IT/OT cybersecurity trends, including the impact of AI, 5G, and edge computing on industrial security.

Future Trends in IT/OT Security

As IT and OT environments continue to converge, the attack surface for cyberthreats is expanding. Organizations must stay ahead of emerging cybersecurity risk while leveraging new technologies to enhance threat detection, resilience, and operational efficiency. Key trends are shaping the future of IT/OT security, including AI-driven security, 5G and edge computing risk, the role of cyber–physical security integration, and evolving regulatory frameworks.

The Rise of AI and ML in IT/OT Security

AI and machine learning (ML) transform cybersecurity operations by enabling real-time anomaly detection, predictive analytics, and automated threat response. In IT/OT environments, AI-powered security solutions can help organizations detect cyberthreats earlier and respond faster via:

- **Anomaly detection**—AI can analyze network traffic patterns and identify deviations that may indicate a cyberattack.
- **Behavioral analysis**—By recognizing unusual behavior, AI-based models can detect unauthorized access attempts and insider threats.
- **Automated incident response**—AI can automatically isolate compromised systems to prevent malware from spreading across IT/OT networks.

However, it is essential to be aware of the challenges present when adopting AI-powered systems, such as:

- **False positives**—AI-based security tools must be fine-tuned to reduce false alarms, particularly in complex OT environments.
- **Data availability**—Many OT systems lack sufficient historical security data for AI model training.
- **Adversarial AI attacks**—Hackers are developing AI-powered cyberattacks, requiring defenders to stay ahead with advanced AI-driven defenses.

Despite these challenges, AI is becoming an essential tool for IT/OT cybersecurity as threats evolve in complexity.

The Impact of 5G and Edge Computing

Adopting 5G and edge computing in industrial environments revolutionizes real-time data processing, automation, and remote operations. However, these technologies also introduce new security risk, such as:

- **Increased attack surface**—More connected devices mean more entry points for cyberattacks.
- **Low-latency networks**—5G enables ultra-fast data transfer, making detecting and stopping cyberintrusions in real time more difficult.
- **Decentralized processing**—With edge computing, data is processed closer to the source, reducing reliance on centralized data centers but creating more security silos.

Mitigating 5G and edge computing risk requires a structured and balanced approach comprising:

- **Zero trust architecture**—Implementing zero trust principles to verify and authenticate every device before granting network access.
- **Secure device authentication**—Using blockchain-based identity verification for IoT and edge devices.
- **AI-driven threat detection**—Leveraging AI-powered security analytics to monitor 5G and edge network activity for suspicious behavior.

As industries embrace 5G-powered smart factories, autonomous transportation, and industrial IoT (IIoT), security teams must integrate robust security controls into these next-generation networks.

Cyber–Physical Security Integration

With the rise of smart infrastructure, industrial automation, and IoT-enabled physical security systems, cyber–physical threats are becoming a growing concern. Attackers can now exploit digital and physical security systems' vulnerabilities to launch cyber–physical attacks.

Some potential scenarios of such risk are:

- **Compromised smart building systems**—Attackers could hack into building automation systems (BAS) to disable alarms, surveillance cameras, or climate controls.
- **Compromised industrial robots**—Cybercriminals could exploit security flaws in robotic manufacturing systems to disrupt production or cause physical damage.
- **Weaponized IoT devices**—Botnets, such as Mirai, have demonstrated how insecure IoT devices can be used for large-scale distributed denial of service (DDoS) attacks.

Securing this new convergence requires controls such as:

- **Integration of IT, OT, and physical security teams**—Security teams must collaborate across disciplines to address emerging threats.
- **Deploying unified security monitoring**—Organizations should invest in security operations centers (SOCs) that monitor cyber and physical threats.
- **Use AI-powered video surveillance analytics**—AI-enhanced cameras can detect unauthorized access attempts and suspicious activity.

As cyber–physical security threats increase, organizations must unify their security strategies across IT, OT, and physical security domains.

The Way Forward

The convergence of IT and OT has become necessary in modern industrial environments, enabling greater efficiency, automation, and real-time decision making. However, this integration introduces an expanded attack surface, exposing critical infrastructure, manufacturing systems, and energy grids to cyberthreats that can disrupt operations, compromise safety, and cause significant financial losses. As organizations continue to merge IT and OT systems, securing these interconnected environments must be a top priority.

Addressing these challenges requires a layered, risk-based security strategy that combines technical, operational, and governance measures. Network segmentation, zero trust principles, real-time monitoring, and secure remote access protocols form the bedrock of this strategy. At the same time, aligning with proven frameworks such as NIST CSF and ISA/IEC 62443 helps organizations standardize their approach, improve resilience, and meet regulatory expectations. Emerging technologies such as AI, 5G, and edge computing will further transform IT/OT security, bringing opportunities and new risk.

Ultimately, securing IT/OT environments is not merely a matter of deploying the right tools. It requires organizational alignment, cross-functional collaboration, and a forward-looking mindset. By breaking down silos, fostering communication between IT and OT teams, and embedding security into every layer of infrastructure and operations, organizations can not only reduce cyberrisk, but build long-term resilience in an increasingly connected industrial world.

Endnotes

1 IOT Analytics, "IT/OT Convergence: The 27 Themes That Define the Future of Industrial Integration," 13 November 2024, *https://iot-analytics.com/it-ot-convergence-27-themes-define-future-of-industrial-integration/*

2 Kerner, S.; "Colonial Pipeline Hack Explained: Everything You Need to Know," 26 April 2022, *https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know*

3 Zetter, K.; "Solar Winds Hack Infected Critical Infrastructure," *The Intercept*, 24 December 2020, *https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/*

4 Marquardt, A.; Levenson, E.; et al.; "Florida Water Treatment Facility Hack Used a Dormant Remote Access Software, Sheriff Says," CNN, 10 February 2021, *https://edition.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html*

5 National Institute of Standards and Technology (NIST), NIST Cybersecurity Framework (CSF) 2.0, USA, 26 February 2024, *https://doi.org/10.6028/NIST.CSWP.29*

6 International Society of Automation (ISA) and International Electrotechnical Commission (IEC), "ISA/IEC 62443 Series of Standards," *https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards*