**Understanding OT Cybersecurity: Safeguarding Industrial Systems and Infrastructure**

**By IsaSecure | March 5, 2025**

Operational Technology (OT) Cybersecurity has become one of the most critical focal points in industrial sectors and critical infrastructure today. As cyber threats multiply and evolve, the need to protect the very systems that power our physical world has never been more urgent. But what makes OT cybersecurity distinct? While information technology (IT) security prioritizes protecting data, OT security is tasked with safeguarding the hardware and software that control physical processes — think of manufacturing plants, energy grids, water treatment facilities and transportation systems.

Understanding OT cybersecurity isn’t just another technical challenge. It’s a transformative journey — one that ties directly into the resilience, safety, and efficiency of the systems that keep our world running. This article offers a working definition of OT cybersecurity as well as a quick summary of its importance in this modern era. It also highlights OT-specific security needs, provides an overview of certain industry standards and certifications and establishes fundamental concepts.

OT cybersecurity is a complex and unique field, but organizations across the supply chain can take concrete steps to mitigate risk.

**The Role of Cybersecurity in OT**

OT cybersecurity can be defined as the measures and practices used to protect OT systems from cyber threats. As OT becomes increasingly integrated with IT networks and exposed to the internet, they also grow more vulnerable to cyberattacks. In the past, many OT environments were isolated (“airgapped”). While the convergence of OT and IT via the industrial internet of things (IIoT) has created new possibilities for sectors like oil and gas, manufacturing, and utilities, it has also expanded the attack surface by many orders of magnitude.

Industrial operations are becoming more reliant on data analytics, artificial intelligence, and machine learning. Unlike traditional IT environments, many OT systems were not originally designed with cybersecurity in mind, making them more susceptible to cyber threats when connected to broader digital networks. As IT/OT convergence increases, cybercriminals have more opportunities to exploit weaknesses in supply chains, remote access points, and legacy systems. Securing advanced technologies against manipulation and cyber threats is crucial.

**Cybersecurity in OT involves practices that aim to:**

1. **Ensure Availability:** Maintain uninterrupted operation of critical systems.

2. **Ensure Safety:** Protect the safety and well-being of the workforce as well as the community and environment. This is a primary concern for OT cybersecurity — see below for a special section on industrial safety.

3. **Protect Integrity:** Prevent unauthorized modifications to system configurations or processes.

4. **Protect Confidentiality:** Safeguard sensitive operational data, although this is often a secondary concern when it comes to OT.

**The Importance of OT Cybersecurity**

Threat actors have begun to target operational technology more frequently in recent years. Securing industrial automation and control systems is crucial for many reasons, including the following.

**Critical Infrastructure Protection**

Many OT systems support essential services. CISA defines the 16 critical infrastructure sectors as the following: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government services and facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportation systems and water/wastewater. These industries are considered so important that their incapacitation would be destructive to society and/or the economy.

A cyberattack on OT systems in critical infrastructure can have widespread consequences —consider the implications of the attack on Colonial Pipeline in 2021. The Colonial Pipeline Company halted operations to limit the attack, causing fuel shortages along the East Coast of the United States.

Or consider the Ukrainian power grid attacks of 2015 and 2016. In 2015, hackers used spear-phishing attacks to gain remote access to supervisory control and data acquisition (SCADA) systems, triggering power outages affecting approximately 230,000 people. In 2016, a similar attack used the Industroyer (CrashOverride) malware to disrupt Ukraine’s power distribution.

Perhaps the most storied example of a cyberattack affecting critical infrastructure is also the first known cyber-physical weapon. Stuxnet was a sophisticated attack that targeted Iran’s uranium enrichment facilities in 2010. A worm caused centrifuges to spin at irregular speeds, leading to physical damage and disrupting Iran’s nuclear program.

OT cybersecurity helps ensure critical infrastructure is protected and mitigates the risk of similar incidents occurring.

**Industrial Safety**

Industrial safety is fundamental to OT cybersecurity. A primary goal of securing OT environments is to protect not only systems and data but also human lives, the environment and physical assets. Cyberattacks targeting OT systems can have dire consequences, such as equipment malfunctions, chemical spills, or even explosions. Strong cybersecurity hygiene helps prevent unauthorized access, system manipulations, and other incidents that could compromise industrial safety.

Cyber threats can lead to hazardous conditions in the real world. For example, the [**Triton/Trisis**](https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/) malware targeted safety instrumented systems (SIS) in a Saudi Arabian petrochemical plant in 2017. Triton was designed to compromise Triconex safety controllers, which are used to shut down industrial systems in case of emergencies. The attackers attempted to manipulate safety protocols, which could have led to catastrophic failures, but the attack was thwarted due to a system malfunction.

With the convergence of IT and OT, the cyber world and the physical world are linked. Cybersecurity concerns are also safety concerns in OT environments. Implementing robust security frameworks, continuous monitoring, and employee training helps ensure that industrial operations remain safe, resilient, and resistant to emerging cyber threats.

**OT-Specific Security Concerns**

Still, operational technology has unique considerations that are very different from IT, and not all stakeholders may fully understand the nuances.

1. **Legacy Systems:** Many OT environments rely on outdated hardware and software that may lack more sophisticated security features commonly found in IT. Upgrading these systems can be expensive and complex and may disrupt operations.

2. **Lack of Patching:** Updates and patches are frequent in IT, but they are often delayed or avoided in OT as the risks to essential functions and safety may be too great.

3. **Visibility:** Monitoring and detection tools compatible with OT environments are often limited in scope, so identifying and responding to threats can be difficult.

4. **Skills Gap:** OT cybersecurity requires expertise in both IT and industrial systems, and there is a critical shortage of professionals with this specialized knowledge — the World Economic Forum reported a shortfall of 3.4 million IT/OT cybersecurity professionals worldwide in 2023.

5. **Complex Environments:** OT networks often involve a mix of proprietary protocols, diverse devices, and geographically dispersed assets, complicating security efforts.

**Relevant Standards and Government Regulations**

Several key standards and government regulations touch upon OT cybersecurity, and it is important to understand what they are and how they interrelate. Examples include:

• **ISA/IEC 62443:** A series of standards that provide guidelines for securing industrial automation and control systems (IACS). These standards emphasize a defense-in-depth strategy and risk-based methodologies to enhance security across all levels of industrial operations. They integrate well with frameworks like NIST CSF (see below) and are often used in conjunction with sector-specific regulations.

• **NIST Cybersecurity Framework (CSF):** A voluntary framework developed by the U.S. National Institute of Standards and Technology to help organizations manage and reduce cybersecurity risks. The NIST CSF aligns with ISA/IEC 62443, providing a broad risk management approach that complements industrial cybersecurity measures.

• **NIS2 Directive:** A European Union directive that strengthens cybersecurity requirements for critical infrastructure operators and digital service providers. NIS2 builds upon the original NIS Directive and mandates enhanced risk management and reporting practices, often aligning with both NIST CSF and ISA/IEC 62443.

• **European Cyber Resilience Act (CRA):** A regulatory framework aimed at enhancing cybersecurity across digital products and services in the EU. It overlaps with NIS2 by setting stringent security requirements for manufacturers and service providers, ensuring resilience against cyber threats.

• **CISA (Cybersecurity and Infrastructure Security Agency):** A U.S. government agency responsible for protecting critical infrastructure against cyber threats and providing guidance on cybersecurity best practices. While it is not a standard or regulation, CISA is worth mentioning here because it frequently references NIST CSF and ISA/IEC 62443 in its recommendations, ensuring that organizations can implement globally recognized standards for cybersecurity resilience.

**The ISA/IEC 62443 Series of Standards**

The ISA/IEC 62443 series of standards, the world’s leading consensus-based automation and control systems cybersecurity standards, is a connecting thread across many of these frameworks. ISA/IEC 62443 sets requirements and processes for implementing and maintaining electronically secure IACS. A horizontal standard that has been proven to apply across industrial sectors, it defines best practices for security and provides a way to assess the level of security performance.

ISA/IEC 62443 establishes that key stakeholder groups share responsibility for OT cybersecurity and must align to ensure the safety, integrity, reliability, and security of control systems. Stakeholder groups include asset owners (end users), automation product suppliers, integrators who build and maintain control system solutions and their components, and service suppliers who support the operation of control systems.

**ISASecure®: Validating Conformance with ISA/IEC 62443**

Validating conformance with these standards is an important part of shared responsibility. The ISASecure® certification program, built around the ISA/IEC 62443 standards framework, is known as the most sought-after certification program by end users. ISASecure provides independent confirmation that products and vendor development processes meet globally recognized security requirements.

**What Is ISASecure? What Does It Do?**

ISASecure is a third-party conformity assessment scheme (also known as a certification scheme) based on ISA/IEC 62443, the accepted gold standard of OT cybersecurity. ISASecure certifies off-the-shelf IACS products, systems, and development practices.

ISASecure has developed the following certifications that leverage ISA/IEC 62443:

• **[Component Security Assurance (CSA) Certification](https://isasecure.org/certification/iec-62443-csa-certification):** CSA focuses on the security of software applications, embedded devices, host devices, and network devices, as defined by the ISA/IEC 62443-4-2 standard.

• **[IIoT Component Security Assurance (ICSA) Certification:](https://isasecure.org/certification/iec-62443-icsa-certification)** Product certification for IIoT devices and gateways.

• **[System Security Assurance (SSA) Certification:](https://isasecure.org/certification/iec-62443-ssa-certification)** All control system requirements in the ISA/IEC 62443-3-3 standard.

• **[Security Development Lifecycle Assurance (SDLA) Certification:](https://isasecure.org/certification/iec-62443-sdla-certification)** Certifies compliance to the ISA/IEC 62443-4-1 standard.

• [**ACS Security Assurance (ACSSA) Program:**](https://isasecure.org/isasecure-site-assessment) The ISASecure site assessment program (still in development) will demonstrate operating site compliance with ISA/IEC 62443.

**Who Benefits from ISASecure?**

Third-party conformity assessment, or certification, is intended to build confidence among IACS stakeholders (owner/operators and product suppliers) that the applicable requirements of ISA/IEC 62443 have been met. The independence of an accredited third-party assessor provides a higher level of trust that the product or process meets the specified requirements.

Asset owners and integration service providers (or system integrators) can procure IACS products that have been designed and developed using the ISA/IEC 62443 security development lifecycle and are capable of meeting the technical requirements of ISA/IEC 62443. Product suppliers can improve product security through independent assessment of their products and security development lifecycle, and improve product recognition via the use of ISASecure certifications in product marketing.

**What Is the Impact of ISASecure?**

ISASecure certifications offer a rigorous and straightforward way to demonstrate that products:

• Meet legislative and regulatory policy requirements.

• Meet requirements mandated by insurance companies.

• Meet asset owner procurement requirements.

Leveraging the wisdom of the entire industry as well as decades of research and development, ISASecure helps decrease cyber risk around the world.

**OT Cybersecurity Keeps Our World Running**

Operational technology cybersecurity is integral to safeguarding modern industrial and critical infrastructure. By protecting the systems that underpin physical processes, stakeholders can help ensure safety, reliability and resilience in the face of evolving cyber threats. While challenges such as legacy systems, skills gaps and complex environments persist, the guidance of well-established standards and certification programs can help improve security posture. The digital and physical worlds continue to enmesh themselves, and the integrity and resilience of the supply chain will come to rely even more on the implementation of robust OT cybersecurity measures.

**Further Reading**

**•** [**Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems (.pdf)**](https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf)

**•** [**Explore ISASecure Certifications**](https://isasecure.org/certification)

**•** [**Secure and Certify Products to ISA/IEC 62443**](https://isasecure.org/certification/certify-now)

***Ready to enhance your OT cybersecurity? Contact us to learn more or view*** [***our certifications***](https://isasecure.org/certification) ***to see how ISASecure can help protect your industrial systems.***