Protecting industrial control systems from advanced cyber threats

A comprehensive defense strategy that pairs cybersecurity and functional safety in every layer of the system

As the industrial and manufacturing sectors continue the shift from centralized to decentralized operations, the world of production as we know it will change completely. This new era, commonly referred to as the fourth industrial revolution or Industry 4.0, is characterized by—smart manufacturing processes where a plethora of intelligent machines, systems, and networks independently exchange and respond to information to manage production. There is a lot to gain with this “smart” production model – in fact, the German government has launched a strategic initiative called INDUSTRIE 4.0 to become a world leader in innovative, internet-based production technology and services.¹ But connecting assets through wired and wireless networks comes with significant risks, demanding tailored cybersecurity and functional safety solutions that help protect physical safety, systems, and private information.

The Rise of Automation and the Industrial Internet of Things

The industrial and manufacturing sectors are experiencing a complete transformation thanks to the rise of the Industrial Internet of Things (IIoT) and smart automation. Disparate assets are no longer the norm, as companies increasingly implement systems that connect all components through wired and wireless

PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ADVANCED CYBER THREATS

Networks. This level of connectivity helps companies:
- Easily control and monitor assets remotely;
- Optimize efficiencies and achieve cost savings;
- Perform preventative diagnostics to predict failures;
- Improve scheduled maintenance routines; and
- Quickly detect and address any faults.

Moreover, the benefits of connectivity can be quantified. Data from GE illustrates that bringing together digital technology and industrial expertise can achieve a 20 percent performance increase.\(^2\) These benefits are contributing to the growth of the global market for industrial control and factory automation, which is expected to grow steadily at a compound annual growth rate (CAGR) of 7.4 percent between 2017 and 2023, from its current value of USD 145 billion.\(^3\)

The "connectivity" trend will not stop anytime soon. Gartner calculated that around 8.4 billion connected devices were in use in 2017, up 31 percent from 2016.\(^4\) Gartner also predicts the number of connected devices to reach 20.4 billion by 2020.\(^5\)

Do the Risks Outweigh the Benefits?

As these markets grow, the cost of a unit or product goes down, impacting profit margins in the process. So while growing markets present abundant opportunities, risk management and third-party certification become essential to help ensure a product is designed right the first time to avoid costly re-works while contending with competition.

The other risk to consider is that, while connectivity can produce efficiencies, industrial control system (ICS) assets are vulnerable to cyber-attacks. Because ICSs are vital to the operation of critical infrastructure, such as our power grids, they are consistently targeted by sophisticated hackers. A breach of any of these systems can have dire consequences, not only to the businesses that operate them, but also their customers and surrounding communities.

Yet forsaking connectivity is not really an option. It is redefining the way modern-day business is conducted, and adapting to this new norm is critical. Companies that change too slowly or miss opportunities can fall behind. For example, Fortune magazine compared FORTUNE 500 firms listed in 1955 versus those listed in 2014. Nearly 90 percent of companies on the 1955 listing are now gone, many because they did not adapt.\(^6\)

Those who have embraced connectivity recognize the importance of cybersecurity, including companies in the industrial sector. The ICS security market size is expected to grow from USD 10.24 billion in 2017 to USD 13.88 billion by 2022, at a CAGR of 6.3 percent.\(^7\) This investment is spurred by the rising number of cyber incidents targeting critical infrastructure and industrial

---


\(^5\) Ibid.


facilities. An analysis of over 24 ICS cyber incidents since 2000 revealed that in exactly half of the cases, attackers sought to violate availability of these systems, disrupting normal industrial functions and operations – and causing severe damage.\(^8\) It comes as no surprise then that 69 percent of ICS security practitioners surveyed in North America consider the threat to ICS systems to be high or severe/critical, and nearly half of those surveyed say their ICS security budgets have increased from the past year due to the nature and frequency of these threats.\(^9\)

These investments are a positive sign that industries are prioritizing safety and security in order to properly reap the benefits of Industry 4.0. But this white paper will demonstrate that ICS cybersecurity solutions need to be tailored to address these systems’ complex, multi-layered, and multi-functional properties for adequate protection. This would involve cybersecurity evaluation of each connected ICS component, paired with functional safety evaluation, to ensure safety systems meet all applicable requirements to help avoid physical damage and safety risks. And since these system components are connected and interact with each other, a holistic evaluation of the system must also be conducted.

**Comparing the IT/OT Landscape**

Understanding the need for both cybersecurity and functional safety evaluation for networked industrial production requires an examination of the IT/OT environments. In many cases, regular IT cybersecurity programs do not offer sufficient protection for ICS, because its applications control both digital and physical assets – so any malfunction or breach can have a direct impact on the physical world. The health and safety of workers and others nearby can be jeopardized, the environment may also be put at risk, and the businesses operating the system can suffer production losses or have their proprietary information compromised.

Gartner has an 80/20 rule-of-thumb that says 80 percent of the security issues faced by OT are almost identical to IT due to OT adopting IT technologies over time. However, 20 percent are unique, not to be ignored, and critical (this includes people, environment, and assets).\(^10\) As IT systems are mainly focused on storing and maintaining data and information, the security issues ranked in order of priority are:

1. Confidentiality
2. Integrity
3. Availability

On the other hand, the impact of shutting down and restarting OT systems on productivity and safety are significant. This is especially true for hazardous locations industries, as their systems are used in the production and delivery of critical services or handling hazardous materials. That’s why in OT, the security issues are ranked in the following order:

1. Control
2. Availability
3. Integrity
4. Confidentiality

In general, OT reverses the ranking of IT’s security issues, placing control and availability at the top. This is because the availability of these systems is critical for productivity. Control – the added priority – is absolutely critical, because it refers to the operator’s ability to control or change the process to ensure safety.

---


Comparing the IT/OT Common Threats and Security Gaps

Recognizing the different rankings of security issues between IT and OT can help us understand the multiple points of attack in an ICS, system vulnerabilities, and the particular consequences of each type of attack. Sensors, networks, and/or computational systems are the most common targets. At the sensor and network levels, attacks mainly target data. Attacks to computational systems target to insert malware that executes. In recent years, industries have witnessed or experienced the latter.

Some types and examples of ICS attacks include:

- **Advanced Persistent Threat Attacks** – This is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. One example of this was the attack on Ukraine’s power grid in 2015. The attackers planned their assault over many months, first doing reconnaissance to study the networks and steal operator credentials, then launching a synchronized attack against operating systems, which left about 225,000 customers without power temporarily.

- **Phishing and Spear-phishing** – These attacks involve a perpetrator impersonating a known or trusted sender or business to gain access to confidential information or data. An example of this was an attack on a German steel mill, which prevented a blast furnace from shutting down and caused immense physical damage. Dragonfly is another example. This attack targeted U.S. Canadian and European defense and aviation companies by using spam email campaigns and watering hole attacks to spy on, damage, and disrupt operations.

- **Stuxnet** – This is a computer worm that targets the types of ICS commonly used in infrastructure supporting facilities. An example of this is the attack on Iran's nuclear program in which 100,000 computers at 22 manufacturing sites were infected with Stuxnet, resulting in the destruction of 1,000 centrifuges.

- **Triton** – Discovered in late 2017, Triton is a malware attack that targets safety-instrumented systems and is capable of shutting down operations, masking the safety functions, or even triggering unsafe operations.

While these attacks are carried out by highly sophisticated hackers, acknowledging and addressing these common security gaps can go a long way in mitigating the risk of successful hacks. Some of the main security gaps are:

- **The use of off-the-shelf software and hardware, coexistence of legacy and new equipment, and the convergence of OT and IT, which "create vulnerable setups that can be abused by attackers."**

- **Open technologies in industrial and manufacturing networks that are more easily accessed by attackers.**

- **Difficulties in updating and protecting legacy systems from emerging threats. Legacy components have long lifespans, meaning they are built and installed long before these threats emerge and are understood. As they are not originally built to withstand these attacks, these components require purpose-built security solutions.**

---

14 Ibid.
“An organization’s cybersecurity strategy should protect the assets that it deems critical to successful operation. Unfortunately, there are no shortcuts, simple solutions, or “silver bullet” implementations to solve cybersecurity vulnerabilities within critical infrastructure ICS. It requires a layered approach known as Defense in Depth.”

Best Practices in ICS Cybersecurity

According to ICS-CERT,

“It’s a holistic approach that protects all assets and recognizes all of the interconnections and dependencies. This approach is also necessary because of the real world consequences of ICS, and security assessments must account for all possible operating conditions of each system component.

These overarching principles of ICS security are incorporated into various global standards and best practice frameworks. Specifically, the International Electrotechnical Commission (IEC), International Society of Automation, and National Institute of Standards and Technology (NIST) recommend that ICS security should always be part of broader ICS safety and reliability programs at both industrial sites and in enterprise cybersecurity programs. Some elements of their recommended strategies for ICS security include:

- Developing security policies, procedures, training, and educational material
- Addressing security throughout the entire lifecycle of the ICS
  - The IEC 62443 series of standards offers guidance in this area. IEC 62443-2-4 defines requirements for solution providers and system integrators. IEC 62443-4-1 defines the secure development lifecycle for product manufacturers, and IEC 62443-4-2 and 62443-3-3 specify the security requirements for both the product and system
- Implementing a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer
- Separating corporate and ICS networks

---

18 Ibid, pg. 35.
PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ADVANCED CYBER THREATS

- Establishing separate authentication mechanisms and credentials for users of the ICS and corporate networks
- Restricting physical access to ICS networks and devices
- Building redundancies in system components and networks
- Applying stronger controls to safety systems in the ICS to help ensure that they can properly deploy risk reduction measures against major accident hazards
- Designing critical systems for graceful degradation to prevent catastrophic cascading events

The Need to Pair Functional Safety Evaluation and Cybersecurity

An analysis of ICS security best practices reveals that a resilient ICS needs to be evaluated for both safety and security, due to its physical applications and network architecture. This is especially true for equipment with functional safety applications, which benefits from the integration of a cybersecurity management system with the overall safety management system of the equipment under control. This means undertaking fulsome cybersecurity and functional safety evaluations. Understanding why and how these two activities are paired requires knowledge of the basic components of the ICS:

1. Programmable logic controllers, which automate industrial processes (the physical actions performed by the system)
2. Distributed control systems, which remotely monitor processes and field devices

3. SCADA systems, which collect data for the purposes of monitoring field sites over large areas and adjusting controls when required

All of these components are connected through networks, but decisions and actions are taken at the field level where the devices are located, through programmable logic controllers. Due to the complicated structure and various roles of each system component, individual parts of the system need to be evaluated for security and safety, as well as the entire system. The assistance of a third-party testing & certification provider becomes essential.

The cybersecurity services offered by CSA Group® combine well-established expertise in functional safety evaluation with a long history of working with emerging technologies. The solutions are tailored to help customers identify potential issues early in the product design phase, and implement security measures to mitigate potential cyber risk. The solutions are also comprehensive in that they address the responsibilities of each player in ICS. These include the suppliers who design and manufacture control systems, integrators and asset owners who engineer and integrate commercial off-the-shelf products into site-specific systems, and asset owners who operate and maintain those site-specific systems.

CSA Group’s cybersecurity capabilities span the entire product lifecycle (Fig. 1), and include:

- **Gap Analysis**: This service helps customers determine the overall areas of cybersecurity weakness in products or processes, as well as necessary improvements.
PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ADVANCED CYBER THREATS

“The cybersecurity services offered by CSA Group® combine well-established expertise in functional safety evaluation with a long history of working with emerging technologies.”

- **Solution Provider Capability Assessment:** An assessment of a set of cybersecurity related capabilities typically described in a plan or set of policies and procedures. This demonstrates that the vendor performing security services meets the IEC 62443-2-4 requirements while installing and/or integrating a control system at the customer plant.

- **Application of Solution Provider Capabilities Assessment:** An assessment that security services providers use to install and/or integrate a control system, performed in compliance with IEC 62443-2-4.

- **Security Development Lifecycle Assurance (SDLA):** This service helps customers stay ahead of potential security threats by addressing them early in the product lifecycle, before committing to production to ensure compliance with IEC 62443-4-1.

- **Embedded Device Security Assurance (EDSA):** This service helps to provide third-party assurance on the security of embedded devices and its features, as well as the device supplier’s development process, according to the requirements under IEC 62443-4-1 and 62443-4-2.

- **Bench Testing:** This includes testing against the Common Weakness Enumeration (CWE) database, product robustness and resilience against known cyber-attacks, as well as penetration testing, radio frequency testing, and source code analysis.

The comprehensive set of tests and evaluations are based on international standards, ISO 27000 Security Management Standards, IEC 62433 Cybersecurity Standards and NIST Guide 800 series. This helps provide greater assurance that the products being delivered to the market have the highest confidence against the vulnerabilities addressed under these schemes.

To demonstrate functional safety, organizations must show that their systems’ functionality is dependable enough for the level of risk it controls. A functional safety evaluation is required to identify the likelihood of potentially dangerous failures and also verifies that the required corrective or preventive actions are properly integrated into the equipment’s design plan.

Industrial and control systems used for safety systems are both costly and complex, which can pose challenges when companies try to get these systems into the global market. Recognizing these challenges, CSA Group’s evaluation aligns with IEC 61508, the umbrella standard for functional safety of industrial electrical, electronic, programmable electronic devices (E/E/PE) and other safety-related systems. The evaluation provides methods for assessing hazards and risks, establishing necessary safety functions, and defining the appropriate Safety Integrity Level designation to reduce risk to a specified acceptable level.

The evaluation also leverages the CASS scheme (conformity assessment of safety-related systems), which offers assessment templates that can be used to “map evidence of compliance to the relevant clauses from IEC 61508 and record the assessor’s evaluation of that evidence.”

---


---
PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ADVANCED CYBER THREATS

“While functional safety helps to ensure that a system is able to detect a potentially dangerous condition and deploy a corrective/protective device or mechanism to avoid hazardous events, cybersecurity helps ensure that these industrial systems, which leverage IIoT, are adequately protected from cyber-attacks that target the systems’ physical functions.”

The Big Picture

When it comes to industrial control systems, cybersecurity evaluation becomes a necessary extension of functional safety. While functional safety helps to ensure that a system is able to detect a potentially dangerous condition and deploy a corrective/protective device or mechanism to avoid hazardous events, cybersecurity helps ensure that these industrial systems, which leverage IIoT, are adequately protected from cyber-attacks that target the systems’ physical functions. Only when both of these evaluations are combined can an organization get a complete picture of the safety and security of its ICS.

22 Ibid.