Cybersecurity Compliance: An Industry-wide Call to Action

by Gary Williams, Senior Director, Cybersecurity Services Offer Leader

Cyberattacks now target industrial control and safety systems.
What you need to do now to mitigate risk.

schneider-electric.com

Life Is On | Schneider Electric

Cyberattacks in the IIoT era

As new threats and incidents emerge, concerns about cyberattacks in the era of the industrial internet of things (IIoT) are escalating—and extending across industries and society. Attackers are now directly targeting industrial control and safety systems. Given that these industrial systems are used across critical global infrastructure and manufacturing, the risks to the people, communities, and environments they serve are real and significant.

While most attacks on industrial control systems to date, such as Stuxnet, are highly sophisticated and targeted, data indicates that they are becoming increasingly easier to execute. As recent reports have shown, attackers are exploiting poor site security practices to introduce malware into control systems.

As cyberattacks become more innovative and aggressive, we, as an industry need to take aggressive measures to prevent them. Vendors, companies, and government agencies alike must come together as a unified industry to address these dangerous threats. Solving the industrial security challenge necessitates close collaboration from all parties. It requires a multi-faceted approach, with each entity playing a key role:

1. **Control systems providers** must reinforce commitments to continually building-in the strongest cybersecurity available and to educating end users on what they need to do to adhere to security best practices at their sites.
2. **End users** must implement and follow the guidelines and instructions vendors provide within their product documentation and prescribed security best practices. Maintaining cybersecurity hygiene is the responsibility of all Operations professionals regardless of what industry or type of facility they operate.
3. **The entire industry** must make a renewed commitment to stronger cybersecurity best practices, standards, and technology across all industry segments—and work together to address this serious issue.

Only when the problem is addressed from all three sides will we be able to effectively mitigate cybersecurity threats. Here is what you need to know.

1. IEC62443/ISASecure compliant devices reduce cost, time, and risk

Schneider Electric has invested heavily to develop security-certified control and safety system products that reduce complexity, increase defense in-depth and mitigate threats from other layers of the plant's network architecture. The result is a more secure control system and OT architecture.

In the age of the IIoT, connectivity is everywhere. Cheap sensors have given even the "dumbest" assets more intelligence. To ensure operators benefit from the information these assets provide, manufacturers are learning to connect them. All that connectivity has increased the risk for cyber incursion. To combat that threat, Schneider Electric has built in security *at the device level*. Five of our global R&D laboratories have received the ISASecure Security Development Lifecycle Assurance certification to ensure our cybersecurity-certified devices are designed to withstand

attacks, provide resilience against unauthorized network activity, and act as a filter to ensure only authorized data traverses between operational layers.

Almost every distributed control and safety instrumented system vendor builds a demilitarized zone (DMZ) between layers 4 and 3 of the ISA99 Purdue Model (Figure 1). The purpose of the DMZ is primarily to protect your operations from threats posed by connectivity to the corporate network. The DMZ is often used to host the Active Directory Server for role-based active control; a Windows service update server, which provides OS updates; and anti-virus servers, and other devices. Each component plays an important role in protecting your operational environment.

For example, the FCP280 and FDC280 controllers within the EcoStruxure Foxboro DCS have been designed and built with Cybersecurity from concept to delivery. Each has undergone a communications robustness test and is certified to ensure compliance with the ISASecure/IEC62443 Embedded Device Security Assurance criteria. When a customer employs a controller that is ISASecure EDSA-certified, the resulting architecture includes an extra layer of defense that can mitigate threats presented by the compromise of components in lower levels of the Purdue Model.

The controller is designed and tested to ensure that it will only accept the protocols, data types, and connectivity it has been designed to accept. Anything else will be ignored. The result is another layer of defense that is tailored to the device location within the architecture.

Now let's add to the architecture a TUV/ISASecure-certified safety instrumented system, such as the Schneider Electric EcoStruxure Triconex process safety system. In accordance with the Purdue Model, the SIS is **below** the defense layer 0 (Figure 2).

Imagine a wireless device in layer 0 being compromised, misconfigured, or flooding the network with erroneous data. Both the protection below layer 0 (SIS) and layer 1 (PLC) will restrict any unauthorized network activity from reaching the Control Room.

The value of IEC62443/ISASecure compliance is quickly realized in the event of an attack, compromise, or even an audit. Research shows that compliance reduces cost, time, and risk. Compliance also helps the client respond to threats, plan upgrades, and generally improve the security posture of your system.

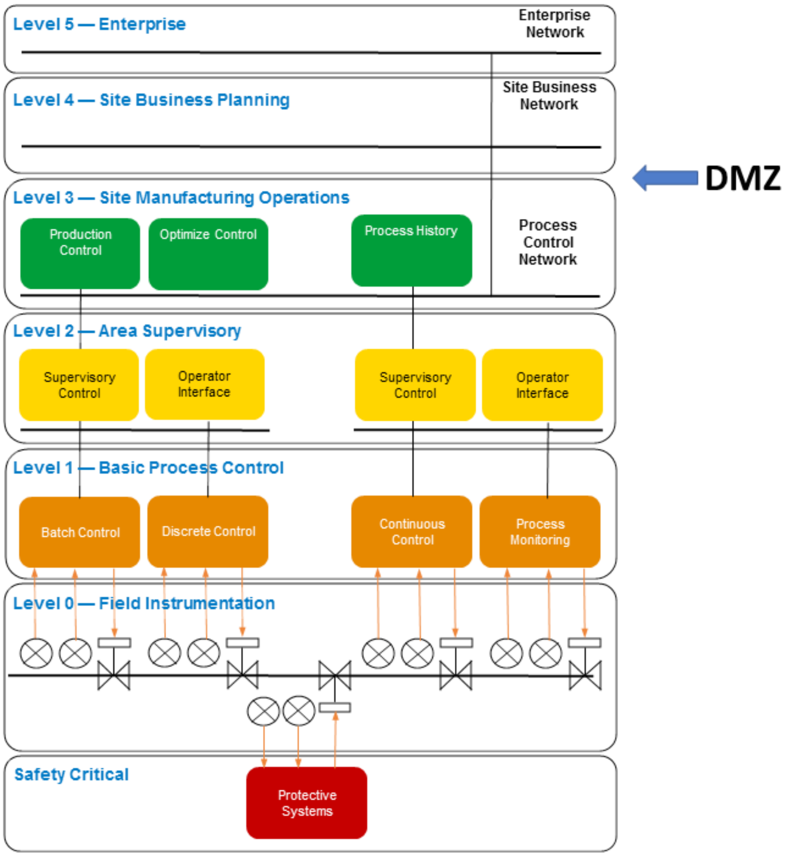

Fig 1 – Cybersecurity addressed at two levels.

Certified devices increase layers of defence

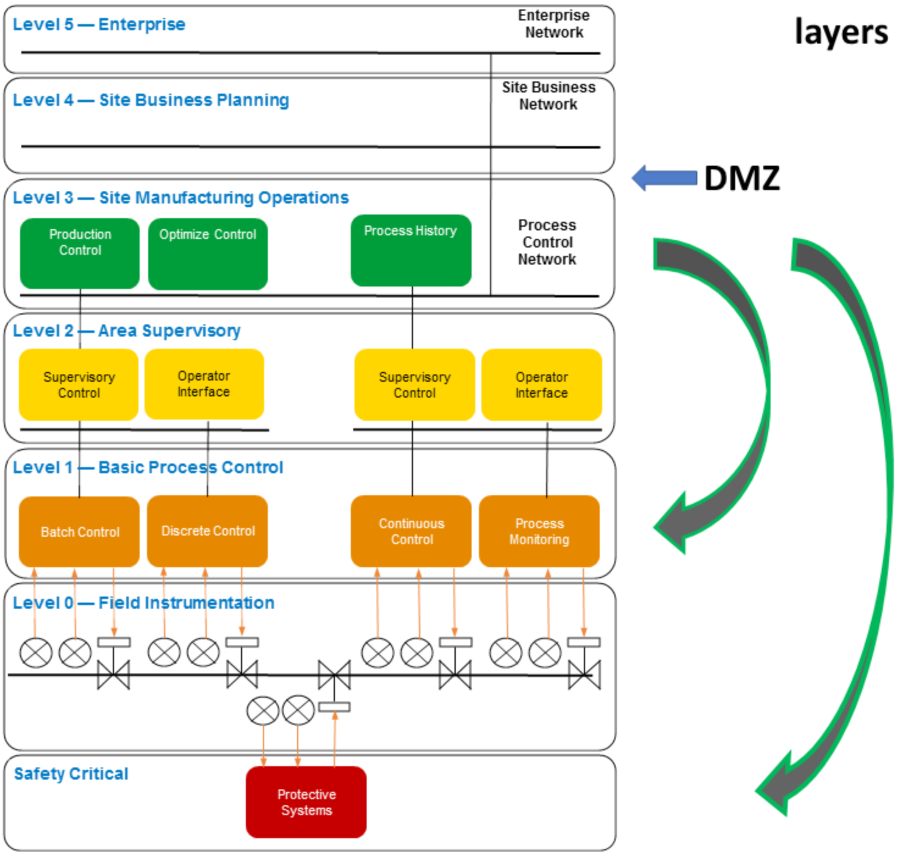

Fig 2 – Cybersecurity addressed at three levels.

Selecting the right components and systems is key to maximizing security and mitigating risk. But strengthened device security alone isn't enough.

2. Plant cybersecurity hygiene protects everyone

Those responsible for industrial operations must also play their part to ensure they are fully protecting their automation systems. This means ensuring security is part of their operations lifecycle by:

- Strengthening and following site security practices by regularly reviewing cybersecurity posture, policies, procedures, and practices
- Applying and maintaining the documented procedures provided by systems, solutions, and software suppliers.
- Becoming educated on current industry cybersecurity standards, and then implementing and strictly adhering to those standards.
- Working with suppliers to ensure that new and evolving threats are addressed holistically, not just by entities that suffer an attack.
- Practicing stronger employee training and heightened personnel screening requirements.
- Mitigating risks presented by legacy products, systems, operating systems, and networks.

The devices mentioned thus far are components of a system. However, there is little value in employing security-compliant devices if the hosting architecture is not hardened. Hardening a system is done according to a risk. Each system should undergo a risk and threat assessment, followed by a gap analysis. These methodologies will produce a prioritized list of weaknesses in the architecture that need to be addressed.

One important cybersecurity best practice end users should follow is the "zones and conduits" approach to network architecture. Both IEC62443 and ISA99 extol the virtues of network segmentation based on your risk model. The practice of segmenting your architecture into zones and conduits results in a better understanding of your network, protects high-risk assets from exploitation, and reduces maintenance overhead.

For example, let's assume you have six Windows XP machines on your network. That operating system is no longer supported by Microsoft. Oftentimes, refineries do not have the opportunity to upgrade these machines until the next scheduled shutdown. These can take place every three to five years. As such, the risk pertaining to these machines increases by the day.

A conduit is the communications link between two zones. Zoning legacy machines protects the zone by mitigating the risks via the conduits, those lines of connectivity between the zone of high-risk assets and other portions of the network. For example, the WannaCry malware exploits weaknesses in a protocol called Server Message Blocks. For the malware to be effective, it must use Ports 137, 138, 139, and 445. Therefore, the Windows XP zone can be protected from this malware by ensuring that Ports 137,138, 139, and 445 cannot be accessed via the conduits. If required, the ports/protocol can be used *within* the zone; however, risk is reduced as connectivity *external* to the zone is filtered.

Another value to network segregation is that it reduces the time needed to respond to and mitigate an attack. If a site is attacked, the forensic investigator employed via the company's incident response needs to isolate the affected system. If a site were to have an open network, the investigator would be forced to shut down the entire operation to isolate the malware or virus and prevent it from spreading. However, if the network is segregated into zones and conduits, the investigator needs to only isolate the zone where the threat was introduced. The conduits will prevent propagation of the threat.

This has been tried and tested. If an operator introduces a threat to a zone by using an unauthorized USB key or if a visiting contractor plugs in an infected laptop, the investigator needs to only isolate the infected zone since the point of ingress and the architecture is already separated.

Zones and conduits, in conjunction with certified devices, can also drastically reduce the time and cost of conducting an audit. For example, auditing a refinery is daunting. Traditionally, the auditor is expected to take five percent of the assets as a sample when conducting an audit. An open architecture makes this very difficult because it is hard to ascertain which assets are most critical. Often an audit can take up to six weeks of onsite activity. However, if the site has applied zones and conduits to its network architecture, the auditor can quickly identify the most critical assets. It's easy to identify five percent of the assets within a zone. Furthermore, assets that have an ISASecure/IEC62443 security certification, like the EcoStruxure Foxboro DCS, reduces the requirement because the certificate proves compliance.

3. An industry-wide call to action

Our industry is conservative and continues to take the "if it ain't broke, don't fix it" approach, but we must change that tactic to prevent the kinds of cyberattacks that could have catastrophic consequences, the likes of which we've not seen before.

Cybersecurity isn't a destination; it's a journey. Security can never be viewed as a one-off project. New threats, attack techniques, and technologies are continually being developed, requiring that security protocols be regularly reviewed and updated.

In the face of increasingly bold, innovative attacks, perpetrated by malicious actors who have unlimited time, resources, and funding, this problem isn't limited to a single company, industry, or region. It's an international threat to public safety that can only be addressed and resolved through collaboration that goes beyond borders and competitive interests. *Everyone* in this industry is responsible for cybersecurity. Every vendor, end user, third-party provider, and systems integrator need to take part in open conversations and drive new approaches that allow installed and new technology to combat the highest level cyberattacks in the IIoT era.

Learn more

EcoStruxure Foxboro DCS is an innovative, fault-tolerant and highly available system that is cybersecurity hardened. It consolidates critical information and elevates staff capabilities to ensure flawless, and continuous plant operation.

For more information about compliance for your critical infrastructure that integrates seamlessly between manufacturing operations and corporate information technology networks, contact **Schneider Electric Cybersecurity** (cybersecurity-services@schneider-electric.com). The Schneider Electric Cybersecurity Service Team addresses an organization's compliance and cybersecurity challenges from analysis through to implementation and management. The team is vendor agnostic and will work with clients to achieve compliance for any system.

Life Is On | Schneider Electric

schneider-electric.com

Schneider Electric
35 rue Joseph Monier
92500 Rueil-Malmaison, France
Tel : +33 (0)1 41 29 70 00