Honeywell
THE POWER OF CONNECTED

Connected Plant

PLCS AND CYBERSECURITY

Addressing Both Information Technology and Operational Technology

White Paper

Abstract

While connectivity within a facility brings significant benefits in terms of efficiency, reliability and even safety, it increases vulnerabilities. Implementation of regulatory standards decreases the risk of successful cyber breaches that can result in unplanned downtime and significant regulatory penalties. The ISA 62443 series of standards provides a good basis for cyber security in industrial control system environments. Compliance with the standard is overseen by the ISASecure program, run by industry consortium ISA Security Compliance Institute (ISCI). While the number of systems that have achieved the ISASecure standard is increasing, when it comes to programmable logic controllers (PLCs), only one commercially available PLC has achieved certification against ISA62443 with ISASecure to date.

Table of Contents

The Growing Challenge

Most operators are well aware of the cybersecurity risks facing industrial control systems. Honeywell's research shows that more than half (53%) of industrial facilities have already experienced a breach[1]; three quarters say they expect an attack on their industrial control system (ICS) in the future.[2]

A number of factors contribute to the growing challenge. First, there is a worldwide shortage of cybersecurity expertise – particularly on the operational technology side, exacerbated by an ageing and retiring workforce. Capgemini's Digital Transformation Institute has highlighted a significant cybersecurity talent gap.[3] Those combining skills in both IT and OT (operational technology) cybersecurity are rarer still.

More significantly, increasing digitization and connectivity in industrial control systems has greatly increased the potential targets for cyber attack. As open standards such as Ethernet and web technologies have become ubiquitous in industrial control, cybersecurity risks have ballooned.

At the facility level, an increasing number of elements within industrial control systems, such as devices, sensors and subsystems are now connected. This connectivity brings significant benefits in terms of efficiency, reliability and even safety, but it also increases vulnerabilities. Meanwhile, connections to industrial control systems from remote workers, partners and customers has increased, also raising risks. Research for Kaspersky Labs shows that organisations allowing third party access are significantly more likely to experience a cybersecurity breach, with almost two thirds (63%) suffering a breach, against more than one third (37%) of those who did not provide access.[4]

The results of successful attacks have been well demonstrated, with associated risks to uptime, equipment and safety.

---

[1] https://www.securityweek.com/industrial-firms-slow-adopt-cybersecurity-measures-honeywell

[2] https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf

[3] https://www.capgemini.com/resources/cybersecurity-talent-gap/

[4] https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf

Regulatory Expectations Grow

For this reason, when it comes to critical infrastructure, governments are already increasingly prioritizing cybersecurity. Dedicated agencies are tasked with promoting the security of industrial systems: ICS-CERT in the US, The National Cyber Security Centre in the UK, Bundesamt für Sicherhein in der Informationstechnik in Germany, New Zealand's NCSC, Cert in Australia and Q-Cert in Qatar, to name a few.

These agencies all insist on minimum standards for critical infrastructure and often incorporate the ANSI/ISA 62443 series of standards, technical reports, and related information that define procedures for implementing electronically secure ICS and automation. ISA62443 is usually either referenced within the relevant regulation of these national industrial cybersecurity bodies, or included within the guidelines issued to aid compliance.

While regulatory efforts have necessarily prioritized critical national infrastructure, the risks and need to implement robust standards are relevant to all industrial operators, however. First, because the standards themselves require those affected to examine and ensure the security of those in their value chain, effectively requiring similar or identical standards of these business, too. Any organisation affected by a cyber security incident will have to spend significant effort and money to both report the incidents and put in place preventive or corrective measures to satisfy the government agencies in the future.

Second, there are financial benefits in terms of cheaper insurance premiums for those who can show compliance with the standards. The return on investment can therefore be rapid.

Third, those lower premiums reflect an obvious reality: That implementation of the standards decreases the risk of successful cyber breaches that can result in risks to people, the environment and facilities, as well as unplanned downtime and significant regulatory penalties – whether the target is determined to be part of the critical national infrastructure or not.

Average annual losses from cyber breaches for industrial facilities are almost $350,000, and close to $500,000 for larger operators.[5] Financial pressure to improve cybersecurity is therefore common across industrial facilities, from utilities and the oil and gas industry, to car manufacturers and food and beverage businesses.

The Weak Link

Whether an organization is part of the critical infrastructure or not, the ISA 62443 series of standards provides a good basis for cyber security in ICS environments.

Compliance with the standard is overseen by the ISASecure program, run by industry consortium ISA Security Compliance Institute (ISCI). It aims to promote cybersecurity by encouraging industrial control product suppliers to achieve ISASecure certification, proving that their products adhere to specifications derived from open, consensus industry standards.

While the number of systems that have achieved the ISASecure standard is increasing,[6] when it comes to programmable logic controllers (PLCs), only one commercially available PLC has achieved certification against ISA62443 with ISASecure to date.

There are a number of reasons for this lack of progress. One is that PLCs are frequently not part of a primary large network, unlike distributed control systems (DSC), which have at least basic perimeter security. Instead they're often used for stand-alone applications – providing control for a single skid or an individual item of smart equipment that does not form part of the main system. Isolated, small nodes such PLCs are more likely overlooked and neglected when it comes to implementing cybersecurity.

Much of the technology is also dated. PLC designs – and often the actual PLCs on site – can be 15 to 20 years old or older. The designs therefore do not address cybersecurity issues that largely did not exist at the time.

These factors perhaps explain why PLC cybersecurity has been neglected. They are not a justification for this lack of protection, however.

There is little evidence that PLCs face less of a threat from cyber attacks, compared to other control components. The Stuxnet worm that targeted Iran's nuclear power plant – and which is the starting point for many conversations about industrial cyber security – specifically targeted the SCADA and PLC systems at the plant, for instance. Compromising the PLCs, it enabled attackers to collect information on the industrial systems, caused the centrifuges to tear themselves apart and render a fifth of them useless.

5 https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf
6 https://isasecure.org/en-US/End-Users/ISASecure-Certified-Devices

More recently, in 2017, we have seen LogicLocker, the first cross-vendor worm specifically targeting PLCs,[7] lock out legitimate users and "dangerously operate physical outputs".[8] The potential results in terms of safety and costs could be enormous.

In fact, PLCs are frequent targets of attacks, and feature heavily in the incident reports of the national ICS regulators. Yet, only one PLC has achieved ISASecure EDSA (Embedded Device Security Assurance) level two certification under the four levels of security defined by ISA62443 (Table 1).

Every other device on the market has not even reached level one – meaning they do not even have protection against coincidental or casual security violations. This perhaps explains why we see incidents such as a connected coffee machine disrupting industrial PLCs.[9]

Table 1: The four levels of security under ISA62443

Level 1	Protection against casual or coincidental violation
Level 2	Protection against intentional violation using simple means
Level 3	Protection against intentional violation using sophisticated means
Level 4	Protection against intentional violation using sophisticated means with extended resources

Even if the PLC controls secondary system, this lack of security is a mistake. For a start, allowing access to the PLC in a highly connected plant, could provide the potential for this to be used to access the DCS. Even where this is not the case, the applications PLCs control, such as boilers, steam generation or heaters in plants' utilities sections are actually essential for the facility. Successful breaches can jeopardise the entire operation.

Recognizing this risk, some plants will, as a result, implement basic security measures on the external network, such as external firewalls. This is an additional cost, however, and is less effective than embedded security.

The problem is likely to only become more pressing: As levels of cybersecurity around the DCS or other central control systems improve, PLCs that remain easy targets will become increasingly attractive to attackers. Those that fail to protect them could be inviting trouble.

Embedded Security

Part of the reason vendors have been slow to adapt their PLCs to the risks of cybersecurity is that it requires a fundamental overhaul of both the design and manufacture of the devices.

To achieve ISASecure EDSA (Embedded Device Security Assurance) Level 2 certification, Honeywell's ControlEdge™ PLC was required to meet ISA 62443 standards both for the embedded device security requirements, detailed in ISA62443-4-2, and the product development requirements in ISA62443-4-1.

In practice this means that, first, the development process provides a certified secure development lifecycle to ensure security is built in from the start, with a trusted supply chain and trusted hardware. Special Honeywell Parts numbers for the PLC components from suppliers and genuine device assurance guard against counterfeit devices being sold on the market or compromised parts making it into devices.

Second, the device has three key embedded security measures:

- A built-in firewall with port filtering, rate limiting and flow control, to protect against denial of service attacks and unauthorised access. It controls network traffic and stops disruptions to the PLC's operation.
- A Secure Boot function provides hardware root of trust with signed firmware and download verification to prevent unauthorized firmware or software from being copied onto the hardware, preventing malware installation. In the event of an operating system (OS) verification failure, the PLC will automatically reboot with a clean copy of the OS.
- Secure communications through IPsec protocols provides a secure communication tunnel for PLC systems communicating with other devices such as engineering work stations, asset management systems, or panel HMIs. This prevents man-in-the-middle attacks and unauthorized access, with communication locked down and requiring explicit enabling for configuration, ModBus, HART-IP and OPC UA communications.

7 https://www.theregister.co.uk/2017/02/15/logiclocker_scada_ransomware/
8 https://www.theregister.co.uk/2017/02/15/logiclocker_scada_ransomware/
9 https://www.tripwire.com/state-of-security/ics-security/how-a-smart-coffee-machine-infected-a-plc-monitoring-system-with-ransomware/

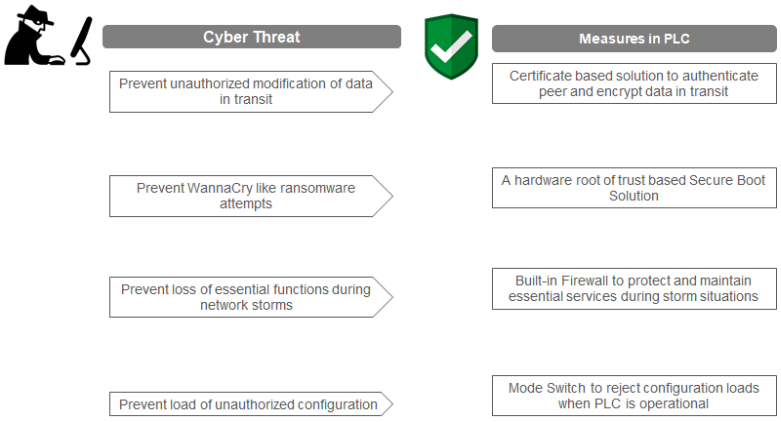

Figure 1: Cyber security protection in layers

These protections guard against and mitigate not only casual or coincidental violations of security (Level 1 under ISA62443) but also intentional attacks (Level 2). They prevent unauthorized modification of data in transit; installation of ransomware and other malware; loss of essential functions during network storms; and loading of unauthorized configurations.

In short, they provide the protections that are increasingly required by regulators and held to be essential for control systems by all operators who are serious about cybersecurity. As the threats continue to evolve and grow, operators will increasingly demand that PLCs demonstrate the same standards with ISASecure certification.

For More Information

Learn more about Honeywell Products and Solutions visit www honeywellprocess.com or contact your Honeywell Account Manager, Distributor or System Integrator.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road,
Zhangjiang Hi-Tech Industrial Park,
Pudong New Area, Shanghai 201203

www.honeywellprocess.com

WP-18-09-ENG
September 2018

Honeywell