WHITE PAPER

Securing Your Industrial Automation Systems Using IEC 62443-4-2 Industrial Computer Host Devices

George Y Hsiao
Product Manager, Moxa IPC Business

MOXA®

Executive Summary

Building an industrial automation system from numerous components supplied by different vendors is no small feat. Ensuring that each individual component that goes into a system, as well as the system overall is secure, can make an already challenging task more painful. IEC 62443-4-2 certification for highly customizable host devices ensures that your open edge computing platform is secure by design.

Large industrial enterprises, system integrators, and independent software vendors all have their own unique pain points when it comes to constructing an industrial automation system. This white paper discusses the particular security challenges these stakeholders face and recommends specific best practices for adopting IEC 62443-4-2 host devices as secure IIoT edge computing gateways for industrial automation systems.

Market Observations

Securing the Edge Computing Environment

As the saying goes, "a chain is only as strong as the weakest link." Taking a holistic approach to making today's industrial automation systems secure and reliable is essential to ensuring no weak links exist in mission-critical applications. As different protocols, standards, and equipment must work seamlessly together in order to deliver the desired results and return on investment, overcoming discrete pain points has become major job duties for industrial automation system managers. One such perennial pain point is securing the system throughout its lifecycle. From planning to deployment, and from maintenance to performing upgrades, a typical automation system requires that all interconnected controls, sensors, machines, processors, and networks reach exacting security standards to maintain system integrity.

Released on March 3, 2023

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

As the industrial automation and control field moves toward distributed computing, computation and data storage are located much closer to the sources of data. As such, edge computing benefits from making processing and decision-making more responsive to time-sensitive and/or location-sensitive requests. Thanks to its proximity to field sensors and control, it can also enable real-time, low-latency processing of data and virtually instant decision-making. As computing is performed on edge host devices, built-in safeguards at every level are critical to system security and integrity. While each system component has separate security standards that protect it from intrusions, attacks, and breaches, it is equally important that system-wide security standards and frameworks offer the same trusted level of protection to the edge computing environment and industrial automation and control applications.

IEC 62443 certification has become the universally recognized go-to standard for industrial automation and control systems. Part 4 of IEC 62443 contains two categories of accreditation on product standards, namely, IEC 62443-4-1 and IEC 62443-4-2. Product manufacturers must first pass the IEC 62443-4-1 accreditation, which covers the product development requirements, in order to be eligible for proceeding to IEC 62443-4-2 certification, which covers technical security requirements for industrial automation and control system components, including embedded devices, network devices, software applications, and host devices. IEC 62443-4-2 host device standards ensure that the entire platform—hardware and operating system—meet the security requirements throughout the system's life cycle. IEC 62443-4-2 certification's rigorous technical requirements are highly sought after as the Industrial Internet of Things continues to make inroads into optimizing industrial automation and control operations and are expected to become mandatory in many countries to promote productivity, efficiency, and resilience for production lines and critical infrastructure.

Why IIoT Applications Need IEC 62443-4-2-certified Host Devices

The deployment of IIoT software on host devices creates an IIoT edge computing gateway that connects industrial automation and control systems to the cloud, so it requires a heightened focus on the security of both the network and edge devices to guarantee secure data transmission. A security-enabled host device is crucial to safeguard the IIoT software deployed on it. When a host device—hardware and software—has been tested and validated to meet IEC 62443 security standards, it reduces the manpower, time, and resources required from OT system integrators, asset owners or managers to validate the security of the device before deploying their IIoT software. As expansive and distributed IIoT systems are becoming commonplace in a variety of outdoor or indoor edge computing applications, host devices such as industrial computers are also designed to be rugged to withstand harsh environments and secure to protect themselves from cyberthreats or tampering.

Security Pain Points for OT Stakeholders

IT or R&D in Large Industrial Enterprises

Large industrial enterprises boast large or multiple IIoT systems to perform different tasks. Different hardware and software components have varying security capabilities. Without a set of common security standards, the burden of testing and validating each component falls on the personnel integrating or operating the system, and the cost and time are borne by the asset owners or end users. Therefore, the benefits of IEC 62443 certification for edge computing devices are obvious. First and foremost, it allows for easy product selection as certified products demonstrate compliance with the rigorous security standards demanded by IIoT systems of today and tomorrow.

In addition, large industrial enterprises face operational challenges that demand a higher level of built-in security. The first challenge is securing the actual edge computing host devices that run the operating system and software applications for the IIoT system. Although IEC 62443-4 certification for host devices has been available for several years, most suppliers only offered certified embedded and network devices. Host devices have typically been open platforms that allow customers to freely configure settings and install additional applications. As a result, ensuring the security of host devices is a significant challenge. In January 2023, the world's first IEC 62443-4-2 certificate was awarded to an industrial computer—Moxa's UC-8200 Series, which closed an important market and product gap in the OT field.

The next challenge of OT systems in large industrial enterprises is deployment of devices in remote locations. IIoT gateways are more vulnerable to tampering or other physical security breaches when they are deployed in unattended or remote areas. Physical security apparatuses, such as barriers or casing secured by locks alone, might not be enough. Moreover, in remote locations, connectivity to the cloud and network availability may be limited. Oftentimes, the only available network is LTE and is less secure than wired connections. Widely recognized as the most rigorous security standards to date, having IEC 62443-4 certification for edge computing devices adds another layer of security when physical security and wireless connectivity are used for remote or unattended deployments.

Lastly, unlike IT systems, OT system components generally have longer life cycles, and IIoT applications are no exceptions. IEC 62443-4 certification is designed to cover the IIoT system's entire life span, often outlasting the life cycles of individual components. When OT professionals choose host devices to connect the IIoT systems to the cloud, they naturally choose products that are built to last, and security certification standards should also go along with the products' longevity.

System Integrators

System integrators may face the same technical challenges seen in large industrial enterprises. Although IEC 62443-4-2 certification ensures the security of individual components that compose a system, it is also important to consider IEC 62443-3-3 certification, which ensures the overall system's security. Hence, a highly customizable yet secure industrial computer certified by IEC 62443-4-2 can be an ideal solution for constructing secure system components. Additionally, system integrators are often responsible for maintaining IIoT systems, and IEC 62443-4 certified devices can contribute to enhanced stability in the long run. In the event of a failure or downtime, these devices can be swiftly recovered, enabling applications to get back online and operate effectively.

Independent Software Vendors

Independent software vendors have expertise in application deployment, development, and security, but may have limited knowledge and experience in hardware and operating system security. As such, in their professional line of work, they may benefit from falling back on IEC 62443-4 certification as it is the latest go-to set of standards for securing edge computing devices. When they engage in development at the application level, they will know hardware and operating system security are taken care of if the industrial computer they are deploying their application on is IEC 62443-4-2-certified.

Best Practices for Industrial Automation and Control System Security

IEC 62443-4-2 certifies that host devices (as well as embedded devices and network devices) are secure-by-design. Choosing IEC 62443-4-2 host devices for your edge computing platform in an entire system that meets IEC 62443-3-3 requirements can ensure that the entire industrial automation system is also secure. These certifications save OT professionals from spending valuable time and resources on manual testing of individual components, and also ensure that each link in the chain is as secure and strong as it could be.

The world’s first IEC 62443-4-2 certificate for a host device was obtained by Moxa’s UC-8200 Series Arm-based computers. As the first such certified product on the market, UC-8200 Series was developed according to IEC 62443-4-1 standards and is compliant with IEC 624433-4-2 industrial cybersecurity Level 2 standards. Running on the latest Moxa Industrial Linux 3.0 (MIL3) platform, the UC-8200 industrial computer features a suite of secure-by-design hardware and software to protect data and infrastructure from cyberthreats.

The UC-8200 certified platform specifically addresses the increasing demand for IIoT system security, as distributed computing requires superior connectivity and network management to protect against DOS attacks and other such vulnerabilities. UC-8200 industrial computer optimizes LAN and WAN availability by automatically switching between Ethernet, Wi-Fi, and LTE connections, which can minimize downtime. Its automatic system failover allows for speedy system recovery. The MIL3 platform comes equipped with quick backup and restore utilities, as well as automated system recovery features based on an overlay filesystem architecture. This helps to reduce downtime in the event of a security breach, process failure, and file corruption, such as in the case of a power outage during a critical update.

Designed with security in mind, UC-8200 computer incorporates a one-time programmable (OTP) fuse and Trusted Platform Module (TPM) 2.0 technology to establish a hardware-based chain of trust that safeguards the Secure Boot process and software updates. This blocks hackers from taking control of the device during boot time and prevents malicious updates from being used for malware exploitation.

Summary

A chain is only as strong as its weakest link. That is why it is so crucial to ensure that each component within the entire industrial automation system is secure. IEC 62443-4-2 host devices are independently evaluated and provide a secure-by-design open platform for industrial automation systems. Installing IIoT software and applications on these host devices creates an IIoT edge computing gateway that meets the industry's gold standard for cybersecurity. Large enterprises, system integrators, and independent software vendors can all rest assured that host devices independently certified by IEC meet the security requirements their applications demand.

For product information and technical specifications of the UC-8200 Series industrial computer and MIL3, visit the product pages:

UC-8200 Series: https://www.moxa.com/en/products/industrial-computing/arm-based-computers/uc-8200-series
MIL3: https://www.moxa.com/en/products/industrial-computing/system-software/moxa-industrial-linux