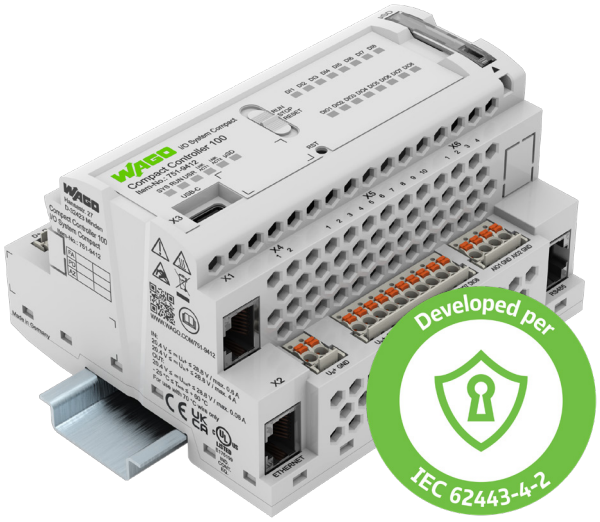
FAQs

Compact Controller 100 Secure



What makes the Compact Controller 100 Secure different from a standard Compact Controller 100?

While the Compact Controller 100 Secure uses the same hardware as the proven Multi I/O controller, WAGO has built the firmware for the Compact Controller 100 Secure around the robust IEC 62443 cyber security standards. These cybersecurity features include encrypted communications, authentication, and network security capabilities designed for connected industrial environments.

It is also built on the Linux® Yocto platform which enables developers to enforce strict system permissions, run background services with non-root privileges, and configure read-only file systems. These security features help reduce cyber risk while supporting remote access and IIoT applications. Customers can deploy connected systems with greater confidence and fewer security gaps. This makes it easier to balance operational performance with cybersecurity objectives.

Does the controller support encrypted communications?

Yes. The controller supports secure communication technologies such as HTTPS, SSH, VPN/IPsec, and SSL/TLS-based communications. Encryption helps protect operational data from interception while it is transmitted across networks. This is especially important for remote access, cloud connectivity, and supervisory control applications. Secure communications also support cybersecurity best practices and compliance initiatives. As industrial connectivity increases, encryption has become a foundational requirement.

Can the controller be securely connected to remote sites or cloud applications?

Yes. The controller supports secure connectivity for remote monitoring, maintenance, and IIoT applications. Secure communication options help reduce risk when exchanging information across external networks. This enables organizations to take advantage of remote access and cloud technologies without compromising security. It also improves visibility into operational assets located in multiple facilities. The result is a more connected and secure automation environment.

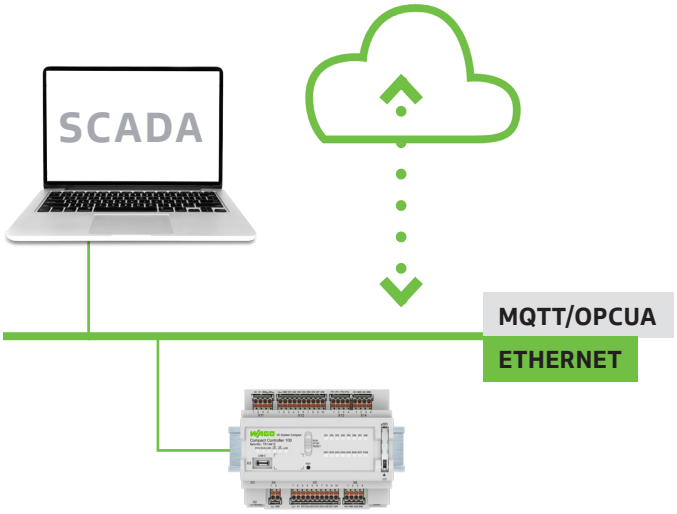
How does the controller help prevent unauthorized access?

The controller uses authentication and access-control mechanisms to help ensure only authorized users can access critical functions. Restricting access reduces the likelihood of accidental changes, unauthorized modifications, or malicious activity. These controls support corporate cybersecurity policies and user-management practices. They are particularly valuable when multiple operators, contractors, or service providers interact with the system. As a result, organizations maintain better control over their automation assets.

Does the controller include firewall functionality?

Yes. The Compact Controller 100 Secure includes firewall capabilities designed to help restrict unauthorized network traffic. Firewalls reduce the attack surface by limiting unnecessary communications. They can also help support network segmentation and cybersecurity policies. This is especially valuable in connected

industrial environments with multiple networked devices. Built-in firewall protection adds another layer of defense without requiring additional hardware.



How does the controller support industrial cybersecurity best practices?

The controller supports secure communications, authentication, access control, and network segmentation strategies. These capabilities align with defense-in-depth principles widely used throughout industry. By combining multiple layers of protection, organizations can reduce exposure to cyber threats. The controller also supports secure deployment in modern OT and IIoT architectures. This helps organizations strengthen overall cybersecurity resilience.

Is the controller suitable for critical infrastructure applications?

The controller is designed for industrial automation, infrastructure, utility, energy, and IIoT applications where cybersecurity is important. Its security-focused capabilities help support reliable operation in connected environments. Organizations responsible for critical processes often require stronger cybersecurity controls. The Compact Controller 100 Secure provides features that help address those requirements. It can therefore be considered for applications where security and availability are priorities.

Does the controller support industrial protocols?

Yes. The Compact Controller 100 Secure supports industrial communications including OPC UA, Modbus TCP, MQTT, and other protocols. These technologies enable interoperability between devices, software platforms, and enterprise systems. Because of its built-in security features, it enables secure deployment options to help protect data while maintaining connectivity with industrial protocols. This allows organizations to support digitalization initiatives with greater confidence. Customers benefit from both flexibility and security.

Can IT and OT networks be separated?

Yes. The controller includes dual Ethernet ports that support network architectures separating operational and enterprise traffic. Network segmentation is an important cybersecurity best practice. Separating environments can help limit the spread of threats and reduce risk. It also simplifies security management and monitoring efforts. This design supports collaboration between IT and OT teams.

How are security updates and firmware managed?

Organizations should maintain firmware updates as part of a broader cybersecurity program. Regular updates help address vulnerabilities and improve security capabilities. WAGO provides firmware and support resources to assist customers. Establishing a documented update process can improve cybersecurity hygiene. Keeping systems current is one of the most effective ways to reduce cyber risk.

Does the controller support secure remote maintenance?

Yes. Technologies such as SSH and VPN connections can be used to support secure remote access. These tools help authorized personnel troubleshoot and maintain systems from remote locations. Encryption protects communications against interception and tampering. This reduces the risk typically associated with remote maintenance activities. Organizations can improve responsiveness without sacrificing security.

Is cybersecurity built into the hardware or added later?

Cybersecurity capabilities are integrated into the Compact Controller 100 Secure from the beginning. This security-by-design approach helps address risk earlier in the system lifecycle. Organizations do not need to rely solely on external devices to add basic protections. Built-in security can simplify deployment and architecture decisions. It also provides a stronger foundation for long-term cybersecurity strategies.

How can customers maximize cybersecurity when deploying the controller?

Because system security is not achieved through any singular product, customers should follow established cybersecurity best practices when deploying any industrial device. This includes using strong passwords, limiting access, segmenting networks, and monitoring activity. Encrypted communications should be enabled whenever possible. Organizations should also keep firmware up to date and maintain backups. Combining these practices with built-in security features creates a stronger overall defense.

Has the Compact Controller 100 Secure been designed for modern IIoT environments?

Yes. The Compact Controller 100 Secure has been designed to meet IEC 62443-4-2 requirements. This security-by-design approach combines industrial control functionality with secure networking capabilities and IIoT-ready communications. It supports digital transformation projects that require connectivity and data sharing. Security features help reduce risks associated with connected systems. This allows organizations to pursue modernization initiatives with greater confidence. The result is a platform designed for current and future industrial requirements.

What is the Cyber Resilience Act (CRA)?

The Cyber Resilience Act is a European Union regulation focused on products with digital elements. It establishes cybersecurity expectations throughout the product lifecycle. Requirements address topics such as secure development, vulnerability management, and security updates. The goal is to improve cybersecurity across connected products and supply chains. Organizations should understand the CRA as cybersecurity requirements continue to evolve.

Why should industrial customers care about the CRA?

The CRA encourages manufacturers to adopt security-by-design practices and maintain vulnerability management programs. Customers benefit from greater transparency regarding cybersecurity capabilities and support. Stronger product security can help reduce operational risk throughout a facility. It may also influence future procurement and supplier-selection decisions. Understanding the CRA helps organizations prepare for changing cybersecurity expectations.

What is IEC 62443?

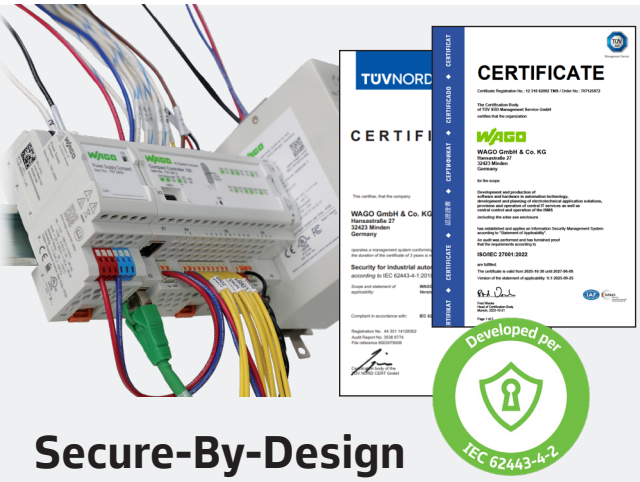
IEC 62443 is a globally recognized series of industrial cybersecurity standards. The standards focus on securing Industrial Automation and Control Systems. They provide guidance for manufacturers, integrators, and asset owners. Topics include risk management, system architecture, secure development, and component security. Many organizations use IEC 62443 as a framework for improving cybersecurity maturity.

How does IEC 62443 differ from the CRA?

IEC 62443 is a voluntary technical cybersecurity certification while the CRA is a regulatory mandate. The certification provides detailed guidance on implementing security controls. The CRA establishes legal requirements for products placed on applicable markets. Many organizations use IEC 62443 practices to support broader CRA readiness efforts. Together they help strengthen industrial cybersecurity programs.

How can CRA and IEC 62443 benefit end users?

Both the CRA and IEC 62443 help improve confidence in connected industrial products. They encourage stronger security practices, improved vulnerability management, and better lifecycle support. Organizations benefit from reduced operational risk and enhanced resilience. These frameworks can also support procurement requirements and cybersecurity initiatives. Ultimately, they contribute to safer and more dependable industrial operations.



Secure-By-Design

Developed to Meet Global Standards:
ISO 27001, Cyber Resilience Act (CRA), & IEC 62443-4-1 & -2

Secure Operating System (OS):
- Secure Boot, TPM 2.0 Support
- Unique Device Certificate from the WAGO Device PKI
- RBAC and LDAP/Active Directory Support
- Central Certificate Store
- Firewall, Ipsec, File Encryption

What is IEC 62443-4-2?

IEC 62443-4-2 defines technical security approvals for industrial automation and control system components. It focuses on capabilities such as identification, authentication, confidentiality, and system integrity. The standard helps establish a consistent benchmark for evaluating product security. Achieving IEC 62443-4-2 certification typically takes 6 - 18 months from the formal application through final approval from an accredited certification organization. Manufacturers must complete a product development lifecycle certification (IEC 62443-4-1), demonstrate the necessary security features (secure boot, encryption, etc.) have been in the product design from the beginning, complete a technical evaluation, and pass a final audit. Customers can use IEC 62443-4-2 to compare cybersecurity capabilities across suppliers.

Why is IEC 62443-4-2 important when selecting a controller?

IEC 62443-4-2 provides an industry-recognized benchmark for security capabilities. It addresses areas such as secure communications, access control, and event logging. Evaluating products against these requirements can improve procurement decisions. It helps customers identify solutions designed with cybersecurity in mind. This can reduce risk and improve confidence in connected systems.

Does compliance with IEC 62443-4-2 guarantee CRA compliance?

No. Compliance with IEC 62443-4-2 does not automatically guarantee compliance with the CRA. However, it can provide valuable technical evidence supporting broader cybersecurity efforts. Many of the security principles are complementary. Organizations often view IEC 62443 as a strong foundation for regulatory readiness. Additional requirements may still need to be addressed.

What does security-by-design mean?

Security-by-design means cybersecurity is considered throughout product development rather than added after deployment. Potential risks are evaluated earlier in the lifecycle. This approach can lead to stronger and more consistent protections. It also helps reduce costly retrofits and workarounds later. Ultimately, security becomes a core characteristic of the product.

How does IEC 62443 help reduce cybersecurity risk?

IEC 62443 promotes a structured and risk-based approach to cybersecurity. The framework addresses people, processes, technologies, and system architectures. Following these practices can improve visibility into potential vulnerabilities. It also helps organizations prioritize risk mitigation efforts. The result is a more resilient automation environment.

What questions should customers ask vendors about IEC 62443?

Customers should ask whether products have been certified against relevant portions of IEC 62443. They should also inquire about vulnerability management processes and update policies. Understanding how security issues are identified and addressed is important. Customers may also ask how long security updates will be supported. These conversations provide insight into a vendor's cybersecurity commitment.