WHITE PAPER



Embedded Systems for IEC 62443 Compliance

A Comprehensive Guide to Securing Embedded Computers Used in Operational Technology

Contact

Alex Lai, Business Development Manager

alexx.lai@advantech.com

Content

1. Introduction 3
3. IEC 62443 Standard Overview 5
4. Achieve IEC scheme certification to IEC 62443 with Bureau Veritas 7
Ensuring your readiness for IEC 62443 certification 7
How does Advantech achieve IEC 62443 Scheme step by step 8
Why is the IEC 62443 certification required? 9
5. Leveraging Advantech to Meet IEC 62443-4-2 standard 9
[Hardware Longevity] TPM/TCG2.0 Support 10
[BIOS Bootloader] Secure Boot 12
[Operation System] Windows IoT Enterprise and Ubuntu Pro for Devices version 14
[Security Application] Windows' Bitlocker and Ubuntu's LUKS technology 16
[Security Application] Dual System fail-over, Acronis backup/Recovery and Trellix Application Control 18
[Security Application] Windows UWF and Ubuntu OverlayFS 19
[Lifecycle Management] Advantech DeviceOn Solution 21
6. IEC 62443-4-2 Requirements Lookup Table 24
7. Glossary 30
8. Conclusion 31
9. Contact Us 32

©2025 Advantech Co., Ltd. All rights reserved.

1. Introduction

The increasing interconnectedness of controllers, machines, devices, and sensors in industrial environments brings with it a heightened risk of cyberattacks. As a result, security has become a critical element in the development of industrial control systems to mitigate intentional or unintentional threats. Such threats can lead to severe consequences, including personal injury, equipment damage, supply chain disruptions, environmental impacts, production losses, and regulatory violations, among others. To address these cybersecurity challenges, the industry has responded by creating standards that assist end users and equipment vendors in securing industrial control systems effectively.

One prominent standard in this regard is the IEC 62443 series, which focuses on the security of Industrial Automation and Control Systems (IACS) throughout their lifecycle. This series provides a comprehensive framework for ensuring the robustness of IACS against cyberattacks. Within the IEC 62443 standard, the certification of systems and products demonstrates independent evaluation, free from known vulnerabilities, and a robust architecture for protection against cyber threats. Compliance with these standards also instills confidence in end users, assuring them that the products they employ adhere to higher standards, thereby enhancing employee safety.

Within the IEC 62443 standard, specific requirements and security levels are defined to address varying levels of cybersecurity measures. In this context, leveraging a Secure Element (SE) like Advantech Embedded System with its pre-integrated security features eases the process of compliance with the IEC 62443 component requirements. Advantech Embedded System empowers OEMs to fortify their IoT devices against both logical and physical attacks while future-proofing their systems.

This white paper aims to guide OEMs in understanding how Advantech Embedded System can facilitate the implementation of IEC 62443-4-2 requirements. It presents insights into the IEC 62443 standard, outlines the advantages of leveraging Advantech's embedded system, maps the security requirements to corresponding security primitives, and provides practical examples of how Advantech Embedded System can meet the specific requirements of IEC 62443-4-2.

By following the guidance provided in this white paper, OEMs can enhance the security posture of their industrial control systems, achieve compliance with the IEC 62443-4-2 standard, and effectively safeguard critical infrastructure against cyber threats.

©2025 Advantech Co., Ltd. All rights reserved.

2. How to Use This Document

This white paper is specifically designed for OEMs who are interested in understanding how Advantech Embedded System can facilitate the implementation of IEC 62443-4-2 requirements. To effectively utilize this document, follow the steps outlined below:
Begin by familiarizing yourself with the IEC 62443 standard overview section. This section provides a brief introduction to the IEC 62443 standard, its main concepts, and the significance of IEC 62443-4-2 certification. It sets the foundation for understanding the importance of achieving compliance with this standard.

- Move on to the section titled "Leverage Advantech Embedded System to Meet IEC 62443-4-2 Requirements." Here, you will gain insights into a set of security primitives that can assist in achieving compliance with IEC 62443-4-2. These security primitives provide a common nomenclature to describe security requirements in IoT systems. This section explains how Advantech Embedded System's features align with these security primitives and contributes to meeting specific IEC 62443-4-2 requirements.
- Refer to the "IEC 62443-4-2 Requirements Lookup Table" section. This comprehensive table maps the IEC 62443-4-2 requirements with the associated security primitives. It provides a clear reference point for understanding which security primitives are relevant to meeting specific requirements. By referring to this table, you can easily identify the security features and capabilities of Advantech Embedded System that contribute to meeting each requirement.
- If you come across any unfamiliar acronyms or terms throughout the document, refer to the "Glossary" section. This section provides definitions and explanations of commonly used acronyms and terms, ensuring clarity and understanding as you navigate the white paper.
- By following these steps, you will gain a comprehensive understanding of the IEC 62443-4-2 standard, how Advantech Embedded System aligns with its requirements, and how to effectively leverage Advantech's solution to achieve compliance. The white paper provides practical examples and uses cases to further illustrate the implementation of Advantech Embedded System in meeting the IEC 62443-4-2 requirements.

Throughout the document, you will find valuable insights and guidance to enhance the security of your industrial control systems. It is recommended to refer to this document as a reference point during the implementation and compliance process, allowing you to leverage Advantech Embedded System effectively and secure your critical infrastructure against cyber threats.

©2025 Advantech Co., Ltd. All rights reserved.

3. IEC 62443 Standard Overview

The IEC 62443 standard is a comprehensive series of standards and technical reports developed to assist organizations in mitigating the risk of failure and exposure to security vulnerabilities in Industrial Automation and Control Systems (IACS), Refer Figure 1. This globally recognized standard provides a framework for implementing robust cybersecurity measures throughout the entire lifecycle of IACS.

The IEC 62443 standard is organized into four main categories: General, Policies and Procedures, System, and Component, each addressing different aspects of cybersecurity in industrial environments.

The General category comprises four parts and contains foundational information such as concepts, models, and terminology that serve as the basis for the other categories of the standard. It establishes a common understanding and language for discussing cybersecurity in IACS.

The Policies and Procedures category consists of five parts and provides detailed requirements and guidelines for creating and maintaining effective security processes. This category focuses on factory operations and addresses various aspects such as security risk assessment, security policies, and security awareness programs.

©2025 Advantech Co., Ltd. All rights reserved.

The System category, consisting of three parts, describes the technical requirements for system design and provides guiding principles for implementing and integrating secure systems. This category primarily targets industrial system integrators and covers topics like system architecture, secure development lifecycle, and system security validation.

The Component category comprises two parts and provides technical guidelines for developing secure industrial components or products. This category is specifically aimed at manufacturers of industrial devices and covers topics like secure coding practices, secure communication, and secure firmware updates.

To assess and classify the required protection level, the IEC 62443 standard introduces the concept of security assurance levels. These levels are connected to risk and asset value, and they are organized into tiers, each requiring increasingly stringent measures to be implemented.

The security assurance levels are categorized as follows:

- SL0 (Security Level 0): No specific requirements or security protection requirements.
- SL1 (Security Level 1): Requires protection against casual or coincidental violations.
- SL2 (Security Level 2): Requires protection against intentional violation using simple means with low resources, generic skills, and low motivation.
- SL3 (Security Level 3): Requires protection against intentional violation using sophisticated means with moderate resources, specific skills, and moderate motivation.
- SL4 (Security Level 4): Requires protection against intentional violation using sophisticated means with extended resources, specific skills, and high motivation.

These security levels represent different levels of sophistication and motivation of potential attackers. SL1 and SL2 correspond to threats originating from insiders or intruders with low skills and motivation, while SL3 and SL4 relate to threats from professional cybercriminals, industrial espionage, or state-sponsored malicious actors with high skills and motivation.

The IEC 62443 standard also defines seven foundational requirements (FR1 to FR7) that serve as the basis for implementing protective measures against cybersecurity incidents. These requirements cover areas such as identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability. Depending on the component type, scope, and applicability, specific security requirements are defined, including Component Requirements (CR) and requirements for embedded devices (EDR), network devices (NDR), software applications (SAR), or host devices (HDR).

©2025 Advantech Co., Ltd. All rights reserved.

Understanding the structure and requirements of the IEC 62443 standard is crucial for effectively implementing cybersecurity measures in industrial control systems. This knowledge forms the foundation for leveraging Advantech Embedded System to meet the specific requirements of IEC 62443-4-2, as outlined in the subsequent sections of this white paper.

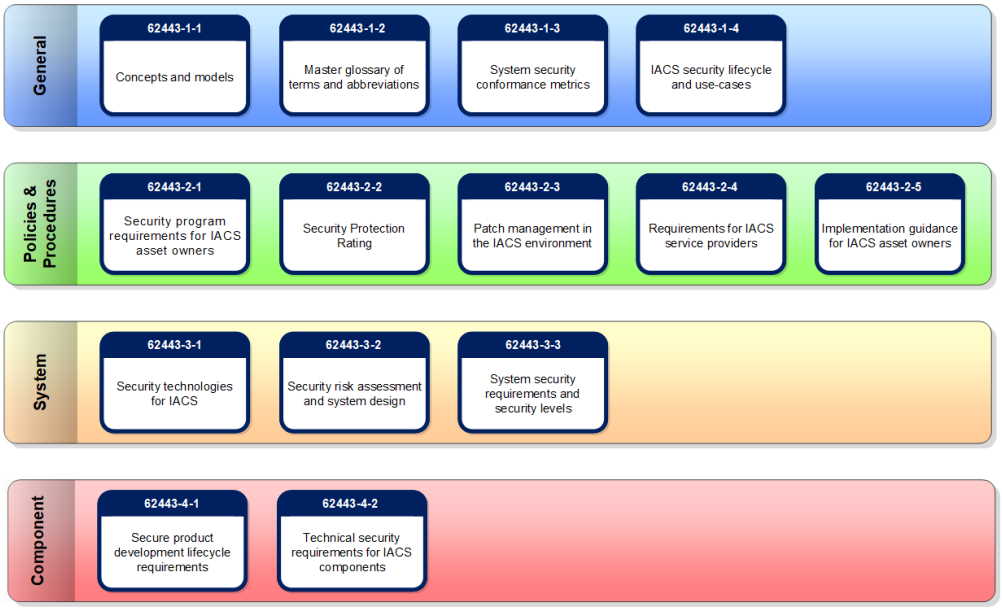


Figure 1. IEC 62443 standard

4. Achieve IEC scheme certification to IEC 62443 with Bureau Veritas

Ensuring your readiness for IEC 62443 certification

Advantech as proudly partnered with Bureau Veritas to offer comprehensive support and services. As experts in cybersecurity, Bureau Veritas has the global information security and cybersecurity certification expertise and industry experience needed to help manufacturers to achieve IT/OT security goals. The specialists in cybersecurity with an expert team already working with organizations to develop effective strategies. A full range of support services to help manufacturers achieve and maintain certification, including (i) evidence collection and analysis, (ii) Audit, interviews and testing, (iii) Assessment and evaluation (iv) Final certification.

In order to minimize OT cyber threats, imagine where your systems are shielded by the highest level of security, where breaches are mitigated before they occur, and where the risk of cyber threats is substantially minimized. Bureau Veritas offers manufacturers the following IEC 62443 services, starting at introductory training, and progressing to full certification.

©2025 Advantech Co., Ltd. All rights reserved.



Figure 2. Bureau Veritas IEC 62443 services from introductory training to full certification (sample)

How does Advantech achieve IEC 62443 Scheme step by step?

Advantech enables organizations to remain compliant with various regulatory requirements that based on IEC 62443, such as those under CRA (Cyber Resilience Act); RED-DA (Radio Equipment Directive Delegated Act), and even more industry standard like SEMI-E187. Ensuring secure and efficient operations across industries. Let us have a look at Advantech's efforts and technological evolution in this area. (refer to Figure 3)

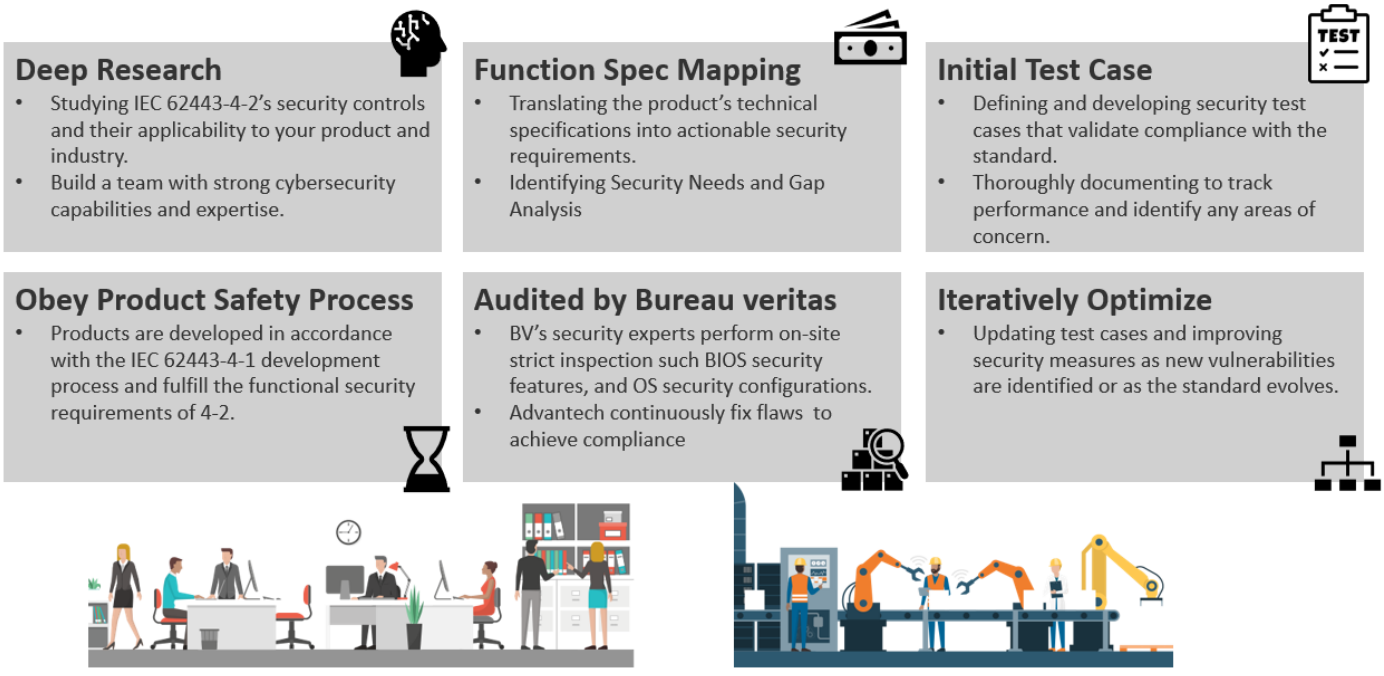


Figure 3. Well-Prepared for IEC 62443 Pre-Certification

©2025 Advantech Co., Ltd. All rights reserved.

Why is the IEC 62443 certification required?

The benefits of IEC 62443 certification are to

- Reduce the risk of cyber-attacks on industrial assets.
- Make more information risk management decisions and provide a defined level of assurance.
- Enhance your company image with stakeholders and differentiate yourself from the competition.
- Cybersecurity standards across different countries are becoming increasingly aligned, with most of them using IEC 62443 as the primary framework for adaptation and development.
- The EU regulation CRA, which will be enforced starting with the 2027 cohort, currently shows a high degree of overlap with IEC 62443.

5. Leveraging Advantech to Meet IEC 62443-4-2 standard

In order to achieve compliance with IEC 62443-4-2 and strengthen the security of industrial control systems, it is essential to leverage advanced technologies and solutions. Advantech Embedded System, with its pre-integrated security features (refer to Figure 4), offers a valuable contribution to meeting the requirements of the standard and ensuring robust cybersecurity measures. By using Advantech devices that have already obtained pre-certification, customers can significantly reduce both cost and time during the secondary development certification process. These Advantech test reports and cybersecurity mechanisms are continuously inspected and updated by BV to ensure ongoing optimization.



Figure 4. Advantech VoC Value and Benefits

©2025 Advantech Co., Ltd. All rights reserved.

The following are key security primitives where Advantech Embedded System offers valuable capabilities. Please refer to Figure 2 to understand the complete architecture.

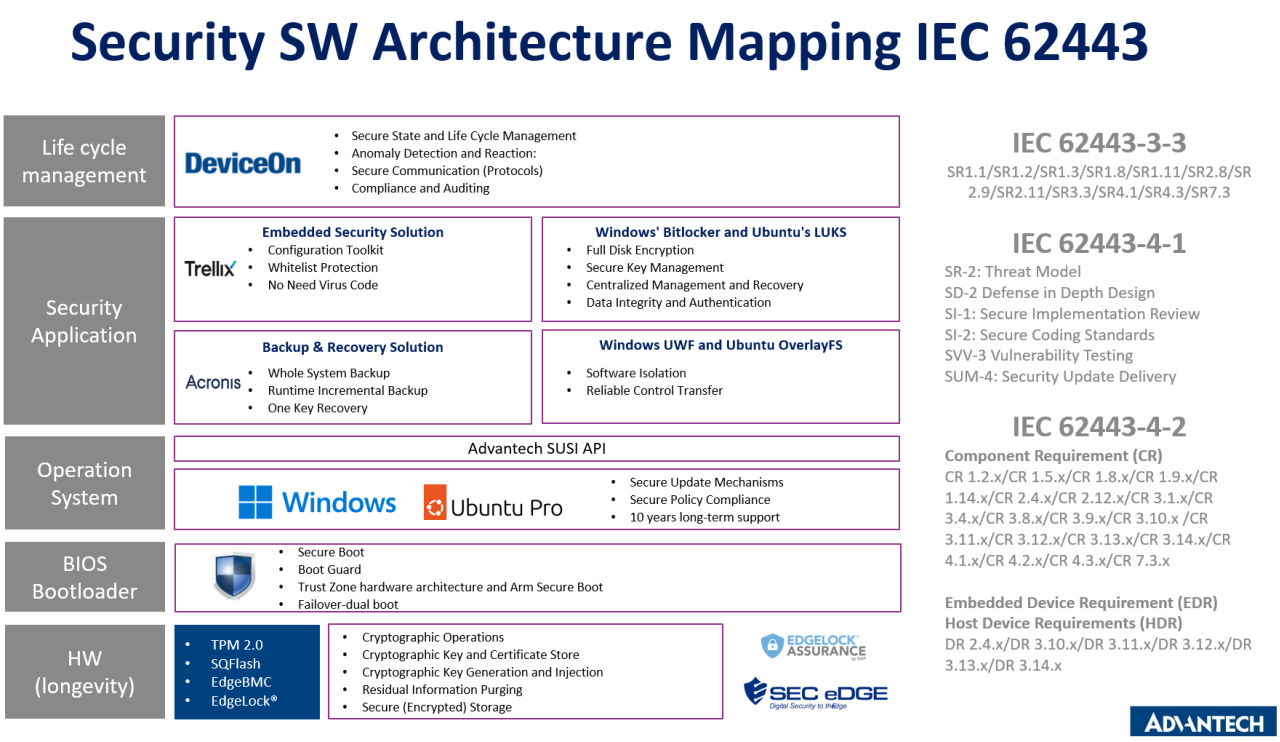


Figure 5. Advantech IEC 62443 SW Architecture

[Hardware Longevity] TPM/TCG2.0 Support

The security primitive of TPM/TCG 2.0 (Trusted Platform Module/Trusted Computing Group) addresses the requirements of cryptographic operations, cryptographic key and certificate management, key generation and injection, residual information purging, and secure storage as outlined in IEC 62443. This primitive utilizes the capabilities of TPM/TCG 2.0 to ensure confidentiality, integrity, and availability of cryptographic assets within industrial control systems.

Features and Benefits:

Cryptographic Operations:

- Secure execution of cryptographic algorithms, including symmetric and asymmetric encryption, digital signatures, and key derivation functions.
- Protection of cryptographic keys and sensitive data through hardware-based isolation and secure storage within the TPM.
- Secure generation of random numbers and secure seed management for cryptographic operations.
- Secure cryptographic protocols, such as secure key exchange and secure communication channels.

©2025 Advantech Co., Ltd. All rights reserved.

Cryptographic Key and Certificate Storage:

- Secure storage and management of cryptographic keys and certificates within TPM.
- Support for various key types, including RSA, ECC, and symmetric keys, enabling diverse cryptographic operations.
- Access control mechanisms to ensure proper authorization for key usage and management operations.
- Protection against key extraction and unauthorized access through hardware-based security measures.

Cryptographic Key Generation and Injection:

- Secure generation of cryptographic keys within the TPM, leveraging its random number generation capabilities.
- Injection of generated keys into the TPM for secure storage and usage.
- Key injection mechanisms to securely import externally generated keys into the TPM.
- Key lifecycle management, including key activation, deactivation, and revocation.

Residual Information Purging:

- Secure erasure of cryptographic keys, sensitive data, and residual information from the TPM to prevent unauthorized access.
- Cryptographically secure erasure techniques, including cryptographic wiping or physical destruction of keys.
- Protection against data remnants and side-channel attacks to ensure the complete removal of sensitive information.

Secure (Encrypted) Storage:

- Secure storage of sensitive data, such as cryptographic keys, certificates, and configuration files, within the TPM.
- Encryption of stored data using TPM-backed keys for confidentiality and protection against unauthorized access.
- Support for secure storage hierarchies and access control policies to enforce data confidentiality and integrity.
- Protection against tampering and unauthorized modifications of stored data.

The TPM/TCG 2.0 security primitive aligns with the requirements of IEC 62443 by providing robust capabilities for cryptographic operations, key management, secure storage, and data protection. By leveraging the TPM/TCG 2.0 technology, OEMs can address the objectives outlined in the standard, including ensuring the confidentiality and integrity of cryptographic assets, secure key management, and protection against unauthorized access or tampering.

©2025 Advantech Co., Ltd. All rights reserved.

TPM/TCG 2.0 provides a comprehensive security primitive for cryptographic operations and key management, enabling the secure generation, storage, and usage of cryptographic assets within industrial control systems. By incorporating TPM/TCG 2.0 technology, OEMs can meet the requirements of IEC 62443 related to cryptographic operations, key and certificate management, residual information purging, and secure storage. This ensures the confidentiality, integrity, and availability of cryptographic assets, strengthening the overall security posture of industrial control systems and protecting against unauthorized access, data breaches, and cryptographic attacks.

[BIOS Bootloader] Secure Boot

The security primitive of Secure Boot technology addresses the requirement of Genuine Identification and Secure Initialization, as outlined in IEC 62443. This primitive ensures the integrity and authenticity of the system's BIOS (Basic Input/Output System) during the boot process, providing a trusted foundation for the entire system operation.

Features and Benefits:

BIOS Secure Boot:

- Verification of the digital signature of the BIOS firmware ensures its authenticity and integrity.
- Prevents the execution of unauthorized or malicious firmware by verifying the cryptographic signature before allowing the boot process to proceed.
- Guards against bootkits, rootkits, and other advanced threats that may attempt to tamper with the system's boot process.
- Provides a secure and trusted initialization of the system, ensuring that only genuine and authorized firmware is executed.

The TrustZone hardware architecture and Arm Secure Boot

The TrustZone is a hardware-based security feature found in many modern processors that provides a secure execution environment called the Secure World and a less trusted execution environment called the Normal World. TrustZone technology is commonly used to implement a secure boot process, ensuring the integrity and authenticity of software components during system startup, often implemented using technologies like NXP's EdgeLock, specifically designed for industrial use cases, strengthens the security of the boot process, ensuring only trusted and verified software is loaded on the device.

©2025 Advantech Co., Ltd. All rights reserved.

Here's a description of how TrustZone and Edge Lock enables a secure boot:

- Secure Boot Process Initialization: the TrustZone features and sets up secure and normal worlds.
- Secure World Initialization: This root of trust is typically a secure boot ROM or a trusted bootloader that is part of the hardware.
- Verification of Boot Components.
- Transition to the Normal World: After the secure bootloader has verified the integrity of the boot components, it transfers control to the Normal World.
- Secure World Isolation: This isolation prevents unauthorized access to secure boot-related operations and protects the secure boot process from tampering.
- Chain of Trust: This process ensures that only trusted and verified software is executed, protecting against the execution of malicious or unauthorized code.
- Secure Boot Policy: TrustZone allows for the establishment of a secure boot policy that defines the criteria for accepting or rejecting boot components.
- Hardware-based root of trust: EdgeLock provides a physically secure and tamper-resistant module that serves as the foundation for the secure boot process.
- Secure storage for keys: EdgeLock securely stores cryptographic keys used for verifying boot components, preventing unauthorized access or modification.
- Tamper-resistant design: EdgeLock's hardware is designed to resist physical tampering, protecting the secure boot process from malicious interference.

By leveraging the hardware-based isolation and security features provided by TrustZone, the secure boot process ensures that the system starts up with verified and trusted software components. This helps defend against various threats, such as bootkits, rootkits, and unauthorized modifications to the system software, establishing a foundation of security for the overall system operation.

Secure Boot plays a critical role in achieving genuine identification and secure initialization of industrial control systems. By implementing these security primitives, OEMs can establish a trusted foundation for the system's operation, protecting against unauthorized or malicious firmware that may compromise the system's integrity. Industrial control systems can confidently defend against boot-time attacks and maintain a secure and resilient operational environment.

©2025 Advantech Co., Ltd. All rights reserved.

[Operation System] Windows IoT Enterprise and Ubuntu Pro for Devices version

The security primitive of Secure Update and Secure Policy Compliance addresses the requirements of secure update mechanisms, secure policy enforcement, and cyber resilience as outlined in IEC 62443. This primitive focuses on the implementation of secure update processes and the enforcement of security policies in Windows IoT Enterprise LTSC and Ubuntu Pro for Devices versions.

Windows IoT Enterprise LTSC is a powerful operating system supported by Microsoft, known for its wide market share and robust features. It provides a secure, reliable platform for IoT devices, with long-term support (LTSC) versions offering 10 years of security maintenance and updates. This ensures that devices remain secure and up-to-date throughout their lifecycle.

Ubuntu Pro for Devices, supported by Canonical, is equally renowned for its extensive market presence and strong security features. It also offers 10 years of security maintenance and updates, ensuring devices are protected against vulnerabilities and receive timely updates. Ubuntu Pro for Devices is designed to provide a secure, reliable environment for a wide range of IoT applications.

Features and Benefits:

Secure Update Mechanisms:

- Utilization of encrypted channels and secure protocols for delivering software updates to IoT devices.
- Verification of the integrity and authenticity of updates through digital signatures or hashes.
- Secure over-the-air (OTA) update processes to prevent unauthorized or tampered updates.
- Timely delivery of security patches, bug fixes, and feature updates to address vulnerabilities and ensure the system's resilience.

Secure Policy Compliance:

- Enforcement of security policies defined by industry standards, regulatory requirements, or organizational guidelines.
- Configuration management to ensure that devices adhere to predefined security policies.
- Continuous monitoring and assessment of device compliance to detect and remediate any policy violations.
- Integration with security information and event management (SIEM) systems for centralized policy management and monitoring.

©2025 Advantech Co., Ltd. All rights reserved.

Cyber Resilience:

- Implementation of proactive security measures to mitigate the impact of cyber threats and incidents.
- Incident response planning and preparedness to minimize downtime and ensure quick recovery.
- Regular backups of critical system components and configurations to enable system restoration in case of compromise or failure.
- Adoption of resilient architectural design principles to enhance the system's ability to withstand and recover from cyberattacks.

The Secure Update and Secure Policy Compliance security primitive aligns with the requirements of IEC 62443 by providing mechanisms to ensure the secure and reliable delivery of updates, enforcing security policies, and enhancing the system's cyber resilience. By incorporating these features into Windows IoT Enterprise and Ubuntu Pro for Devices versions, OEMs can demonstrate compliance with the standard's objectives related to secure update processes, policy enforcement, and maintaining cyber resilience.

Secure Update and Secure Policy Compliance are essential components in achieving the objectives of IEC 62443, focusing on the secure and reliable updating of IoT devices, enforcement of security policies, and enhancing cyber resilience. By leveraging these security primitives in Windows IoT Enterprise and Ubuntu Pro for Devices versions, OEMs can establish a robust foundation for maintaining the security and integrity of industrial control systems. This ensures that devices are updated with the latest security patches, adhere to defined security policies, and are prepared to withstand and recover from cyber threats. By embracing these security practices, industrial control systems can operate in a secure and resilient manner, safeguarding critical assets and maintaining operational continuity.

©2025 Advantech Co., Ltd. All rights reserved.

	Ubuntu (Open Source Community)	Ubuntu form ADVANTECH	Windows IoT form ADVANTECH
Technical support	× No professional technical support Need many engineers to develop	○ Level 1 Support by ADVANTECH Level 2 Support by Canonical	○ Level 1 Support by ADVANTECH Level 2 Support by Microsoft
Official endorsement	× Community forum' s answers can' t be trusted by end customer	○ The answers from Ubuntu official mail can convince customers	○ The answers from Microsoft official mail can convince customers
Other Linux Distribution	× Insufficient support for cybersecurity & AIoT ecosystem	○ Tri-weekly security updates Most popular Linux for IoT, Edge & AI	○ Monthly security updates Most popular cosumer & comercal OS in the world
Long-term support	× Need many engineers to maintain	○ ADVANTECH x Canonical can support	○ ADVANTECH x Microsoft can support
Legal redistribution	× Cannot be used for commercial purposes, only for personal use	○ Legal shipment and professional Opensource consulting services	○ Legal shipment and can get regular online update

ADVANTECH

Figure 6: Advantech-provided operating system comparison table.

[Security Application] Windows' BitLocker and Ubuntu's LUKS technology

The security primitive of secure (encrypted) storage addresses the requirements of IEC 62443 related to the secure storage of data through the utilization of encryption technologies such as BitLocker for Windows and LUKS (Linux Unified Key Setup) for Ubuntu. This primitive focuses on the implementation of secure storage mechanisms to ensure the confidentiality and integrity of sensitive data within industrial control systems.

Features and Benefits:

Full Disk Encryption:

- Integration of BitLocker on Windows and LUKS on Ubuntu for full disk encryption.
- Encryption of the entire storage media, including system and data partitions, to protect against unauthorized access.
- Utilization of strong encryption algorithms (e.g., AES) and secure key management practices for robust data protection.
- Automatic encryption of new data and transparent decryption for authorized users during system operation.

©2025 Advantech Co., Ltd. All rights reserved.

Secure Key Management:

- Generation and storage of encryption keys in a secure manner.
- Integration with hardware-based security modules (e.g., TPM) to enhance key protection and prevent unauthorized key access.
- Utilization of password-based encryption keys or other authentication factors to ensure authorized access to encrypted storage.
- Implementation of key rotation and recovery mechanisms to maintain the security and availability of encryption keys.

Centralized Management and Recovery:

- Integration with centralized management systems for streamlined deployment, configuration, and monitoring of encrypted storage.
- Support for key escrow and recovery mechanisms to prevent data loss in case of key loss or system failure.
- Logging and auditing capabilities to track and monitor encryption-related events and activities.
- Compliance with regulatory requirements and industry standards for data protection and encryption practices.

Data Integrity and Authentication:

- Utilization of cryptographic checksums or digital signatures to ensure data integrity.
- Verification of data authenticity during read/write operations to prevent tampering and unauthorized modifications.
- Integration with secure boot mechanisms to establish a trusted boot process and protect against unauthorized system modifications.

The secure (encrypted) storage security primitive aligns with the requirements of IEC 62443 by providing robust encryption mechanisms through BitLocker for Windows and LUKS for Ubuntu. By leveraging these technologies, OEMs can address the objectives of secure storage, ensuring the confidentiality and integrity of sensitive data within industrial control systems. The integration with secure key management practices and centralized management further enhances the security posture and compliance with IEC 62443 requirements.

Secure (encrypted) storage is a critical security primitive for industrial control systems, and the adoption of technologies such as BitLocker for Windows and LUKS for Ubuntu provides a strong foundation for achieving the objectives of IEC 62443. By implementing full disk encryption, secure key management, centralized management, and data integrity measures, OEMs can ensure the confidentiality and integrity of sensitive data stored within the systems. This, in turn, strengthens the overall security posture, protects against unauthorized access and data breaches, and contributes to compliance with industry standards and regulatory requirements for secure storage practices.

©2025 Advantech Co., Ltd. All rights reserved.

[Security Application] Dual System fail-over, Acronis Backup/Recovery, and Trellix Application Control

The security primitive of reliable control transfer addresses the requirements of IEC 62443 related to ensuring uninterrupted and reliable control of industrial systems through the implementation of dual system fail-over, Acronis backup/recovery, and Trellix Application Control solutions. This primitive focuses on providing continuous availability, rapid recovery, and robust security measures to maintain the integrity and resilience of control processes.

Features and Benefits:

Dual System Fail-over:

- Implementation of redundant control systems with automatic fail-over capability.
- Utilization of hot standby configurations to ensure seamless transfer of control from the primary system to the backup system in case of failure.
- Synchronization of data and state information between the primary and backup systems to maintain operational continuity.
- Real-time monitoring and detection of system failures to trigger the fail-over process and minimize the impact on control operations.

Acronis Backup/Recovery:

- Regular and automated backup of critical control system components, including configuration files, application data, and system state.
- Utilization of incremental or differential backup strategies to optimize storage space and reduce backup time.
- Encryption of backup data to ensure its confidentiality and prevent unauthorized access.
- Rapid recovery capabilities to restore the control system to a known and functional state in the event of data corruption, hardware failures, or other disruptions.

Trellix Application Control:

- Implementation of a comprehensive whitelist solution, such as Trellix Application Control, to control and monitor the execution of authorized software and processes within the control system.
- Creation of a trusted baseline of approved applications, ensuring that only authorized software is allowed to run on the control systems.
- Continuous monitoring and verification of software integrity to detect and prevent the execution of unauthorized or malicious code.
- Protection against unauthorized modifications or tampering of critical control system components.

©2025 Advantech Co., Ltd. All rights reserved.

Continuous System Monitoring:

- Real-time monitoring of system health, performance, and availability to proactively detect and address potential issues.
- Alerting and notification mechanisms to promptly inform administrators about system failures or abnormal conditions.
- Integration with monitoring tools and dashboards to provide comprehensive visibility into the status of control systems.
- Logging and auditing capabilities to track and analyze system events for troubleshooting and forensic purposes.

Testing and Validation:

- Regular testing of fail-over mechanisms, backup/restore procedures, and whitelist configurations to ensure their effectiveness and reliability.
- Simulation of failure scenarios to validate the response and recovery capabilities of the control system.
- Documentation and maintenance of recovery plans and procedures for reference during emergency situations.
- Training of personnel on fail-over processes, backup/restore operations, and whitelist management to facilitate swift and accurate response to system failures.

[Security Application] Windows UWF and Ubuntu OverlayFS

The security primitive for Windows Unified Write Filter (UWF) and Ubuntu OverlayFS addresses the requirements of IEC 62443 related to Software Isolation and Reliable Control Transfer. This primitive focuses on leveraging the capabilities of UWF and OverlayFS technologies to provide software isolation and reliable control transfer mechanisms in industrial control systems.

Features and Benefits:

Software Isolation:

- Windows UWF: UWF enables the creation of a protected overlay that isolates the system's primary disk from write operations. It helps prevent unauthorized changes or tampering with the operating system and applications.
- Ubuntu OverlayFS: OverlayFS allows the mounting of multiple file systems as layers, providing a mechanism to isolate changes made during system operation. It ensures that modifications are isolated from the underlying system, enhancing system integrity and security.

©2025 Advantech Co., Ltd. All rights reserved.

Reliable Control Transfer:

- Windows UWF: UWF provides a reliable control transfer mechanism by allowing the system to be configured in a read-only mode. This prevents accidental or unauthorized modifications to the system configuration, ensuring system stability and control integrity.
- Ubuntu OverlayFS: OverlayFS enables the creation of snapshot-like states, allowing for easy rollback to a known good configuration. This facilitates reliable control transfer by ensuring the system can revert to a stable state in case of errors or unauthorized changes.

Benefits of Software Isolation and Reliable Control Transfer:

- Protection against unauthorized modifications: UWF and OverlayFS technologies safeguard the system's integrity by isolating software changes and preventing unauthorized modifications to critical components.
- Enhanced system stability: By utilizing software isolation mechanisms, the risk of system instability caused by unapproved or faulty modifications is minimized, ensuring continuous and reliable system operation.
- Easy recovery and control transfer: The ability to revert to a known good configuration quickly and reliably simplifies the recovery process and facilitates control transfer between redundant or backup systems.
- Reduced maintenance and downtime: With software isolation and reliable control transfer, organizations can minimize maintenance efforts, reduce downtime, and enhance overall system availability and operational efficiency.

The security primitive utilizing Windows UWF and Ubuntu OverlayFS effectively addresses the IEC 62443 requirements for Software Isolation and Reliable Control Transfer. These technologies provide robust mechanisms to isolate software changes, prevent unauthorized modifications, and ensure reliable control transfer within industrial control systems. By implementing these security measures, organizations can enhance the security and integrity of their systems, mitigate the risk of unauthorized access or tampering, and meet the compliance requirements of IEC 62443.

The security primitive leveraging Windows UWF and Ubuntu OverlayFS for Software Isolation and Reliable Control Transfer offers a robust solution to address the IEC 62443 requirements. By utilizing these technologies, organizations can achieve software isolation, protect against unauthorized modifications, and facilitate reliable control transfer within industrial control systems. The benefits include enhanced system stability, reduced maintenance efforts and downtime, and improved overall system integrity and security. By adopting this security primitive, organizations can strengthen their compliance with IEC 62443 and ensure the secure and reliable operation of their industrial control systems.

©2025 Advantech Co., Ltd. All rights reserved.

[Lifecycle Management] Advantech DeviceOn Solution

The security primitive for Advantech DeviceOn addresses the requirements of IEC 62443 related to (attested) secure state and life cycle management, anomaly detection and reaction, and secure communication (protocols). This primitive focuses on leveraging the capabilities of Advantech DeviceOn solution to ensure the secure and efficient management of industrial devices throughout their life cycle, proactive anomaly detection, and secure communication protocols.

Features and Benefits:

(Attested) Secure State and Life Cycle Management:

- Secure provisioning and onboarding of devices onto the Advantech DeviceOn platform, ensuring their initial configuration and state are protected.
- Secure bootstrapping and cryptographic key management to establish a trusted and authenticated communication channel between devices and the DeviceOn platform.
- Device identity management, including the generation, storage, and management of digital certificates, to enable device authentication and secure communication.
- Life cycle management capabilities, such as firmware updates, patch management, and configuration management, to maintain devices in a secure and up-to-date state.
- Attestation mechanisms to periodically verify the integrity and compliance of device software and configurations, ensuring they remain in a trusted state throughout their operation.

Anomaly Detection and Reaction:

- Real-time monitoring and analysis of device behavior and operational data to detect anomalies, abnormal patterns, or potential security breaches.
- Application of advanced analytics techniques, including machine learning and anomaly detection algorithms, to identify deviations from normal device behavior.
- Automated alerting and notification mechanisms to promptly notify administrators or security teams about detected anomalies or security incidents.
- Integration with incident response workflows enable timely reaction and mitigation actions in response to identified anomalies or security threats.

©2025 Advantech Co., Ltd. All rights reserved.

Secure Communication (Protocols):

- Support for secure communication protocols, such as Transport Layer Security (TLS), to ensure the confidentiality, integrity, and authenticity of data transmitted between devices and the DeviceOn platform.
- Implementation of secure API endpoints and communication interfaces to prevent unauthorized access or tampering of data.
- Encryption of sensitive data, including device configurations, firmware updates, and operational data, during transit and storage.
- Integration with industry-standard security protocols and best practices, such as mutual authentication and secure key exchange, to establish secure and trusted communication channels.

Compliance and Auditing:

- Logging and auditing capabilities to capture and retain a comprehensive record of device management activities, including configuration changes, updates, and security events.
- Support for compliance frameworks, such as IEC 62443, to facilitate adherence to security standards and regulatory requirements.
- Generation of compliance reports and dashboards to provide visibility into the security posture of managed devices and their adherence to security policies.
- Periodic vulnerability assessments and security assessments to identify and address potential weaknesses in device configurations or management processes.

The integration of Advantech DeviceOn as a security primitive effectively addresses the IEC 62443 requirements pertaining to (attested) secure state and life cycle management, anomaly detection and reaction, and secure communication (protocols). By leveraging the robust features of DeviceOn, industrial device management can be carried out securely and efficiently throughout the devices' life cycle. The platform ensures secure provisioning, authentication, and ongoing management of devices, while attestation mechanisms verify the integrity and compliance of device software and configurations. The anomaly detection capabilities enable real-time monitoring and proactive identification of anomalies or potential security breaches, facilitating timely reaction and mitigation. Additionally, the support for secure communication protocols ensures the confidentiality, integrity, and authenticity of data transmitted between devices and the DeviceOn platform. By adopting this security primitive, organizations can enhance their compliance with IEC 62443, improve the overall security posture of industrial systems, and mitigate the risk of unauthorized access or tampering.

©2025 Advantech Co., Ltd. All rights reserved.

By leveraging the advanced security capabilities of Advantech Embedded Systems across these security primitives, OEMs can effectively address the specific requirements of IEC 62443-4-2. These features not only strengthen the security of the IoT devices but also contribute to the overall compliance and certification process, ensuring a robust and future-proof solution.

In the following sections, we will delve into the specific IEC 62443-4-2 requirements and demonstrate how Advantech Embedded System aligns with and supports the implementation of these requirements.

©2025 Advantech Co., Ltd. All rights reserved.

6. IEC 62443-4-2 Requirements Lookup Table

To facilitate the implementation of IEC 62443-4-2 requirements using Advantech Embedded Systems. The following table maps the specific requirements to the corresponding security primitives and features provided by the system:

Security Functional Primitives	Dependency of Security Primitives	Benefiting from Advantech Security Solutions	Requirements
Device attestation	· (Attested) Secure State and Life Cycle Management · Genuine Identification · Secure Initialization · Anomaly Detection and Reaction · Cryptographic Operation	· DeviceOn supported BIOS Secured boot · TPM/TCG 2.0 supported	CR 1.2.0 CR 1.2.1
Secure Updates	· Secure Communication (Protocols) · (Attested) Secure State and Life Cycle Management · Secure Initialization · Anomaly Detection and Reaction · Cryptographic Key and Certificate Storage · Secure (Encrypted) Storage · Cryptographic Operation	· DeviceOn support TLS2.0, Cloud Agent also supported · BIOS Secured boot · TPM/TCG 2.0 supported and BitLocker	EDR/NDR 2.4.1 CR 3.4.0 CR 3.4.1 CR 3.4.2 EDR/NDR 3.10.1 EDR/NDR 3.12.0 EDR/NDR 3.13.0
Secure Onboarding and off Boarding	· Secure Provisioning and Decommissioning · Secure Communication (Protocols) · (Attested) Secure State and Life Cycle Management	· TPM2.0 API Support · DeviceOn support TLS2.0, Cloud Agent also supported · DeviceOn supported · TPM/TCG 2.0 supported	EDR/NDR 3.12 EDR/NDR 3.13

©2025 Advantech Co., Ltd. All rights reserved.

Security Functional Primitives	Dependency of Security Primitives	Benefiting from Advantech Security Solutions	Requirements
	• Genuine Identification • Cryptographic Key Generation and Injection • Cryptographic Key and Certificate Storage • Residual Information Purging		
Secure Provisioning and Decommissioning	• (Attested) Secure State and Life Cycle Management • Genuine Identification • Secure Initialization • Anomaly Detection and Reaction • Cryptographic Key Generation and Injection • Cryptographic Key and Certificate Store • Cryptographic Operation • Cryptographic Random Number Generation • Silicon Root of Trust • Residual Information Purging	• DeviceOn supported • BIOS Secured boot • TPM/TCG 2.0 supported • BIOS Secured boot/ARM Trusted Boot	EDR/NDR 3.12 EDR/NDR 3.13 CR 4.2.0
Secure Communication Protocols	• Cryptographic Key Generation and Injection • Cryptographic Key and Certificate Storage • Cryptographic Operation • Secure (Encrypted) Storage	• TPM/TCG 2.0 supported and Bit locker	CR 1.8.0 CR 3.1.0 CR 3.1.1 CR 3.8.0 CR 4.3.0

©2025 Advantech Co., Ltd. All rights reserved.

Security Functional Primitives	Dependency of Security Primitives	Benefiting from Advantech Security Solutions	Requirements
Secure backup and recovery	· (Attested) Secure State and Life Cycle Management · Cryptographic Key and Certificate Storage · Secure (Encrypted) Storage · Cryptographic Operation	· DeviceOn supported · TPM/TCG 2.0 supported and Bit locker	CR 7.3.1
Secure Initialization	· Cryptographic Key and Certificate Storage · Cryptographic Operation	· TPM/TCG 2.0 supported	CR 3.4.0 EDR/NDR 3.10.1 EDR/NDR 3.14.0 EDR/NDR 3.14.1
Anomaly detection and reaction	· (Attested) Secure State and Life Cycle Management · Secure Initialization · Anomaly Detection and Reaction · Secure (Encrypted) Storage · Cryptographic Operation · System Event Logging · Residual Information Purging · Reliable Control Transfer	· DeviceOn supported · BIOS Secured boot · TPM/TCG 2.0 supported and Bit locker · BIOS WDT recovery, fail-over. Fail back	CR 1.5.1 CR 1.9.1 CR 1.14.1 CR 3.4.2 EDR/NDR 3.11.0 EDR/NDR 3.11.1
Cryptographic Key Generation and Injection	· Cryptographic Key and Certificate Storage · Cryptographic Operation · Cryptographic Random Number Generation	· TPM/TCG 2.0 supported	CR 1.5.0 CR 1.5.1 CR 1.8.0 CR 4.3.0

©2025 Advantech Co., Ltd. All rights reserved.

Security Functional Primitives	Dependency of Security Primitives	Benefiting from Advantech Security Solutions	Requirements
Cryptographic Key and Certificate Store	· (Attested) Secure State and Life Cycle Management · Secure Initialization · Anomaly Detection and Reaction · Secure (Encrypted) Storage · Cryptographic Operation · Residual Information Purging · Software Isolation	· DeviceOn supported · BIOS Secured boot · TPM/TCG 2.0 supported and Bit locker · OverlayFS and UWF	CR 1.5.1 CR 1.9.1 CR 1.14.1
Cryptographic Operation	· Software Isolation	· OverlayFS and UWF	CR 1.8.0 CR 1.9.0 CR 1.14.0 CR 3.1.0 CR 3.1.1 CR 3.4.0 CR 3.4.1 CR 3.8.0 CR 3.9.0 CR 3.14.0 CR 3.14.1 CR 4.1.0 CR 4.3.0 CR 7.3.1

©2025 Advantech Co., Ltd. All rights reserved.

Security Functional Primitives	Dependency of Security Primitives	Benefiting from Advantech Security Solutions	Requirements
System Event Logging	· Secure (Encrypted) Storage · Cryptographic Operation	· PM/TCG 2.0 supported and Bit locker	CR 2.12.0 CR 2.12.1 CR 3.9.0
Silicon Root of Trust	· Cryptographic Operation	· TPM/TCG 2.0 supported	EDR 3.12 EDR 3.13
Protection of Personal Information	· (Attested) Secure State and Life Cycle Management · Secure Initialization · Cryptographic Key Generation and Injection · Secure (Encrypted) Storage · Cryptographic Operation	· DeviceOn supported · BIOS Secured boot · TPM/TCG 2.0 supported and Bit locker	CR 1.5.1 CR 4.1.0
Cyber Resilience	· Secure Updates · Secure Backup and Recovery · Secure Initialization · Anomaly Detection and Reaction · Secure (Encrypted) Storage · Cryptographic Operation · Reliable Control Transfer	· OS LTSC and DeviceOn OTA · Acronis · BIOS Secured boot · DeviceOn supported · TPM/TCG 2.0 supported and Bit locker · WDT, dual-boot, fail-over	

©2025 Advantech Co., Ltd. All rights reserved.

Security Functional Primitives	Dependency of Security Primitives	Benefiting from Advantech Security Solutions	Requirements
Reliable Control Transfer	• Secure Initialization • Cryptographic Key and Certificate Storage • Cryptographic Operation	• BIOS Secured boot • TPM/TCG 2.0 supported	

By referring to this lookup table, OEMs can easily identify which specific security primitives and features of Advantech Embedded System correspond to each requirement of IEC 62443-4-2. This enables a streamlined approach to fulfilling the standard's requirements and leveraging the inherent security capabilities of the system.

In the following sections, we will delve into each requirement in detail, discussing how Advantech Embedded System addresses the specific security needs and contributes to meeting the IEC 62443-4-2 compliance objectives.

©2025 Advantech Co., Ltd. All rights reserved.

7. Glossary

To ensure a clear understanding of the terms and acronyms used throughout this document, the following glossary provides definitions for common terms:

1. **OEM:** Original Equipment Manufacturer. A company that produces and sells devices or components to be used in the products of another company.
2. **IEC 62443:** International Society of Automation/International Electro technical Commission 62443. A series of standards and technical reports that address the security of Industrial Automation and Control Systems (IACS) throughout their lifecycle.
3. **Security Levels (SL):** Security assurance levels defined in the IEC 62443 standard, representing incremental levels of cybersecurity measures and requirements.
4. **Secure Element (SE):** A hardware component or module that provides secure storage, cryptographic operations, and other security functions to protect sensitive data and ensure system integrity.
5. **Security Primitives:** Common nomenclature used to describe security requirements in IoT systems, providing a standardized approach to mapping security features to specific security requirements.
6. **Secure Boot:** A security mechanism that ensures the integrity and authenticity of system firmware during the boot process, protecting against unauthorized or malicious firmware.
7. **Access Control:** The process of managing and enforcing permissions and privileges for users or entities accessing a system, ensuring that only authorized entities can perform specific actions.
8. **Secure Communication:** The implementation of encryption and secure protocols to protect data transmitted between devices, networks, and applications, preventing unauthorized access or tampering.
9. **Security Monitoring:** The continuous monitoring and analysis of security events and activities within a system to detect anomalies, unauthorized access attempts, or policy violations.
10. **Event Logging:** The process of capturing and recording security-related events, providing an audit trail for forensic analysis, compliance reporting, and incident response.
11. **Firmware Updates:** The process of updating the system's firmware with the latest patches, bug fixes, and security enhancements to address vulnerabilities and improve system resilience.
12. **Physical Security:** Measures and mechanisms designed to protect the physical components of a system from unauthorized access, tampering, or theft.

By referring to this glossary, readers can easily grasp the meaning of key terms and acronyms used in the document, enhancing their understanding of the content and facilitating effective communication throughout the white paper.

©2025 Advantech Co., Ltd. All rights reserved.

8. Conclusion

In today's interconnected industrial landscape, cybersecurity is of paramount importance to safeguard industrial control systems against malicious threats. The IEC 62443 series of standards provide a comprehensive framework for addressing the security of Industrial Automation and Control Systems (IACS) throughout their lifecycle.

In this white paper, we have explored how Advantech Embedded Systems can be leveraged to meet the requirements of IEC 62443-4-2, focusing on the key security primitives and features that contribute to achieving compliance. By utilizing Advantech Embedded Systems, OEMs can enhance the security posture of their IoT devices, ensuring protection against logical and physical attacks while adhering to industry-leading cybersecurity standards.

Advantech Embedded Systems offer robust security capabilities such as secure boot, access control, secure communication, security monitoring, firmware updates, and physical security measures. These features align with the foundational requirements of IEC 62443-4-2, enabling OEMs to build secure and resilient industrial control systems.

By incorporating Advantech Embedded Systems into their product development process, OEMs can benefit from pre-integrated security features, saving time and effort in implementing complex security measures. Furthermore, the use of Advantech Embedded System with its compliance to IEC 62443 certification provides end-users with assurance and confidence in the safety and security of their systems.

As the threat landscape continues to evolve, it is crucial for OEMs to prioritize cybersecurity and adhere to industry standards and best practices. Advantech Embedded Systems serve as a valuable tool in this endeavor, offering a reliable and future-proof solution for achieving IEC 62443-4-2 compliance.

In conclusion, by leveraging Advantech Embedded Systems and aligning with the IEC 62443-4-2 standard, OEMs can establish robust security measures, mitigate risks, and deliver industrial control systems that are resilient against cybersecurity threats. By embracing these security practices, we can collectively contribute to the advancement of secure and trustworthy industrial environments.

©2025 Advantech Co., Ltd. All rights reserved.

9. Contact Us

With cybersecurity regulations like EU CRA and IEC 62443 becoming increasingly stringent, now is the time to enhance your security posture. Advantech offers hardware with built-in security value to help you navigate these requirements and succeed. Contact us today to learn more!

Alex Lai, Business Development Manager
alexx.lai@advantech.com

©2025 Advantech Co., Ltd. All rights reserved.