ADVANTECH
Enabling an Intelligent Planet

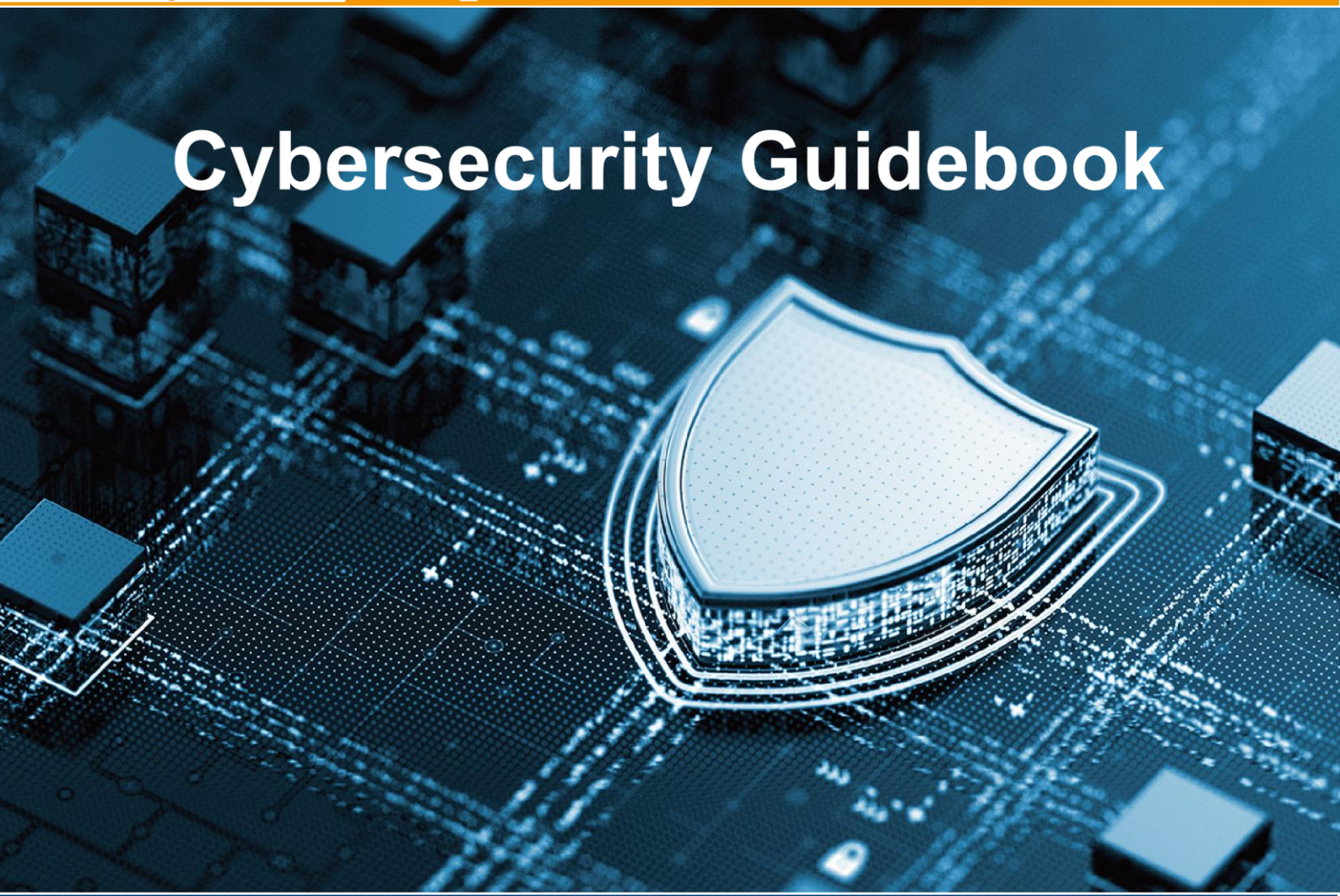
AMC

ADVANTECH iAutomation
Premier Partner

Guidebook

July, 2025 Rev. A3_0701

Cybersecurity Guidebook



Cybersecurity Committee

CONTENTS

1 Introduction

In an increasingly digital world, cybersecurity has become a critical pillar of organizational resilience and trust. As cyber threats evolve in complexity and scale, Advantech adopts a comprehensive approach to safeguard our assets, operations, and stakeholders. This begins with adherence to **Cybersecurity Standards**, which provide globally recognized frameworks for protecting information systems and managing risk. Equally important is **Corporate Governance**, where leadership integrates cybersecurity into strategic decision-making and accountability structures. Effective **Security Management** ensures that policies, processes, and controls are in place to prevent, detect, and respond to threats in a timely manner. Complementing these efforts are **Secure Products** that provide the necessary defense mechanisms against cyber-attacks. Together, these elements form a robust cybersecurity ecosystem, enabling organizations to operate securely and confidently in today's interconnected environment.

Cybersecurity Standards

As cyber threats grow more sophisticated and pervasive, the global regulatory landscape is evolving to ensure stronger protection for critical infrastructure, digital products, and industrial systems. Among the most significant recent developments in cybersecurity standards are the **EU Cyber Resilience Act (CRA)**, the **NIS 2 Directive**, and the **IEC 62443** series. Together, these standards reflect a holistic approach to cybersecurity—combining legal obligations, strategic governance, and technical rigor—to build a more resilient and secure digital environment across both IT and OT domains.

Cybersecurity Governance

Cybersecurity governance ensures that organizations manage digital risks effectively through structured oversight and strategic planning. A **clear organizational structure** defines roles and responsibilities, enabling efficient decision-making. Strong **security policies** guide behavior and set standards for protecting information assets. Robust **security infrastructure** provides the technical foundation to detect, prevent, and respond to threats. Meanwhile, **product security advisories** help maintain trust by addressing vulnerabilities and communicating risks transparently. Together, these elements form a cohesive approach to securing both operations and products in an ever-evolving threat landscape.

Security Management

Security management is a critical function in modern software and system development. Implementing a **Secure Software Development Life Cycle (SSDLC)** ensures that security is integrated from design to deployment, reducing risks early in the process. **SBOM management** enhances transparency by tracking software components and their origins, enabling organizations to identify and respond to supply chain risks. Complementing these practices, **vulnerability management** focuses on the continuous identification, assessment, and remediation of security flaws to minimize exposure. Together, these elements form a proactive approach to building and maintaining secure systems.

Secure Products

Developing a secure product requires a comprehensive approach to embedded cybersecurity. **Compliance with IEC 62443-4-2** ensures that industrial components meet rigorous technical security requirements. Clearly defined **security requirements** guide the design to address potential threats from the outset. Core principles like **AAA (Authentication, Authorization, Accounting)** and **CIA (Confidentiality, Integrity, Availability)** form the foundation of secure system behavior and data protection. Finally, thorough **security testing** validates that implemented controls are effective, ensuring the product can withstand real-world cyber threats. Together, these practices support the development of robust and trustworthy products.

2 Cybersecurity Standards

2.1 ISO/IEC 27001

ISO/IEC 27001 specifies the requirements for establishing and maintaining an Information Security Management System (ISMS). The standard emphasizes a risk-based approach to managing information security, encouraging organizations to identify, assess, and mitigate risks specific to their operational environment. The ISO/IEC 27000 series is built upon the Plan-Do-Check-Act (PDCA) cycle, a methodology aimed at continuous improvement.

While ISO/IEC 27001 sets the baseline for ISMS requirements, other standards in the series provide complementary guidelines and sector-specific recommendations. Together, they form a comprehensive ecosystem that addresses everything from risk assessment and incident management to privacy controls and cloud security.

2.2 Network and Information Systems 2 (NIS 2)

The NIS 2 directive aims to extend the scope of obligations on entities required to take measures to increase their cybersecurity capabilities. The Directive also aims to harmonize the EU approach to incident notifications, security requirements, supervisory measures and information sharing.

NIS 2 is about laws and policies, which mandate that critical infrastructure must have cybersecurity measures appropriate to the threats, and they must report cyber incidents to regulatory authority.

2.3 Cyber Resilience Act (CRA)

The CRA is an EU regulation for improving cybersecurity and cyber resilience in the EU through common cybersecurity standards for products with digital elements in the EU, such as required incident reports and automatic security updates. Products with digital elements mainly are hardware and software whose "intended and foreseeable use includes direct or indirect data connection to a device or network".

For CRA, product manufacturers are required to develop digital products and software that meet certain standards of quality and durability before they can be used by end-users.

2.4 IEC 62443

The IEC 62443 cybersecurity standard defines processes, techniques and requirements for Industrial Automation and Control Systems (IACS). Its documents are the result of the IEC standards creation process where all national committees involved agree upon a common standard. All IEC 62443 standards and technical reports are organized into six general categories: General, Policies and Procedures, System, Component, Profiles, and Evaluation.

IEC 62443 is comparable to the cybersecurity professionals who design and construct security controls and measures. They follow a set of technical standards to ensure every measure effectively controls and measure.

2.5 Combined Impact of NIS 2, CRA, and IEC 62443 in Europe

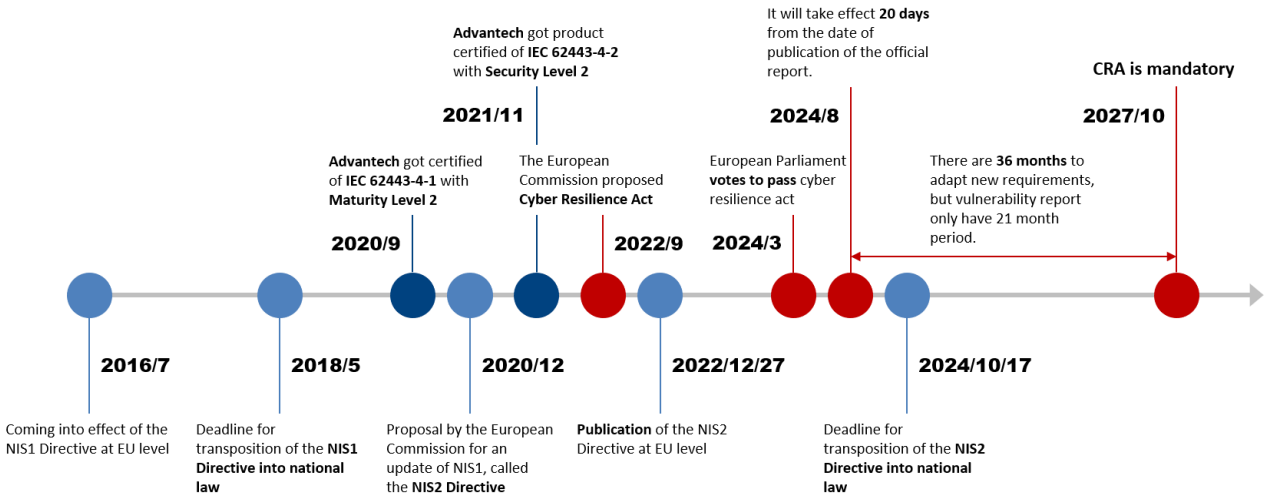
NIS 2 ensures that operators of essential services maintain high levels of security and report incidents, which is crucial for the OT sector's overall resilience.

CRA complements this by making sure that the products used in these sectors are secure from the start, reducing the risk of vulnerabilities.

IEC 62443 bridges the gap by offering technical standards that apply to the specific needs of OT systems, providing a common language and set of practices for industry stakeholders.

	Who is affected?	**Which products/sectors matter?**	**Penalties**
NIS 2	Companies who operate essential or important IT/OT systems	Sectors that are ▪ Essential for society (e.g. energy, transport) ▪ Important ones (e.g. manufacturing chemicals, digital services, food)	▪ Up to 10 million euros or 2% of annual turnover ▪ Personal liability of management
CRA	Manufacturers, distributors and importers of products with digital elements	Software and hardware products with a direct or indirect data connection to another device or network	▪ Up to 15 million euros or 2.5% of annual turnover ▪ Product recalls

2.6 Timeline



Advantech did early research for cybersecurity management and methodology of the products; got certified of IEC 62443-4-1 with Maturity Level 2 on September 24, 2020. A development process is employed to ensure the design/implementation/verification/validation/deployment of a product following the security principles and guidelines.

The best practice of the development process is performed in 2021. Advantech was certified for IEC 62443-4-2 Security Level 2 on the Ethernet Switch product. Advantech met all security requirements defined in IEC 62443-4-2 and executed all development stages that SSDLC employed by following IEC 62443-4-1.

From 2024 to 2027, there are 36 months to adapt new requirements of the CRA. With the understanding that adaptation timelines may vary based on product complexity, supply chain readiness, and regulatory interpretation. Advantech has experience of IEC 62443 and employs product development based on the baselines of each cybersecurity standard. Not only relevant to secure products, but also security governance and management for security activities in enterprise.

3 Cybersecurity Compliance

3.1 Is ISO 27001 enough for NIS 2 compliance?

NIS2 emphasizes cybersecurity from a societal perspective. The scope is the activities that are important for the continuity of the proper functioning of a country. So first and foremost, ensure that the scope of activities that are ISO 27001 certified are all activities that are important or essential to society.

The table below provides a comparison between NIS2 requirements and ISO 27001.

NIS 2 Area	ISO 27001 Controls
Governance (Article 20) Annex A 5.1	Annex A 5.31 Annex A 5.34 Annex A 5.35 Annex A 5.36 Annex A 6.3
Security risk measures (Article 21) **A. Policies on risk analysis and information system security**	5.2 6.1.2 6.1.3 8.2 8.3 Annex A 5.1
Security risk measures (Article 21) **C. Business Continuity**	Annex A 5.29 Annex A 5.30 Annex A 8.13 Annex A 8.14 Annex A 8.15 Annex A 8.16
Security risk measures (Article 21) **D. Supply chain security**	Annex A 5.19 Annex A 5.20 Annex A 5.21 Annex A 5.22 Annex A 5.23

NIS 2 Area	ISO 27001 Controls
Security risk measures (Article 21) **E. Security in network acquisition, development and maintenance**	Annex A 5.20 Annex A 5.24 Annex A 5.37 Annex A 6.8 Annex A 8.8 Annex A 8.9 Annex A 8.20 Annex A 8.21
Security risk measures (Article 21) **F. Policies and procedures to assess effectiveness**	9.1 9.2 9.3 Annex A 5.35 Annex A 5.36
Security risk measures (Article 21) **G. Basic cyber hygiene practices and training**	7.3 7.4 Annex A 5.15 Annex A 5.16 Annex A 5.18 Annex A 5.24 Annex A 6.3 Annex A 6.5 Annex A 6.8 Annex A 8.2 Annex A 8.3 Annex A 8.5 Annex A 8.7 Annex A 8.9 Annex A 8.13 Annex A 8.15 Annex A 5.19 Annex A 5.22
Security risk measures (Article 21) **H. Policies and use of cryptography and encryption**	Annex A 8.24

NIS 2 Area	ISO 27001 Controls
Security risk measures (Article 21) **I. Human resources security**	Annex A 5.9 Annex A 5.10 Annex A 5.11 Annex A 5.15 Annex A 5.16 Annex A 5.17 Annex A 5.18 Annex A 6.1 Annex A 6.2 Annex A 6.4 Annex A 6.5 Annex A 6.6
Security risk measures (Article 21) **J. Use of multi-factor authentication**	Annex A 5.14 Annex A 5.16 Annex A 5.17
Reporting (Article 23)	Annex A 5.14 Annex A 6.8
Use of European cybersecurity certification schemes (Article 24)	Annex A 5.20

Business Continuity Management

Advantech establishes and maintains a business continuity mechanism to effectively control the potential risks and minimize their impact on the company, safeguarding the interests of customers and stakeholders. To ensure the effective operation of the business continuity management system, Advantech has established a Business Continuity Management Committee. The committee has formulated business continuity management policies, conducted business impact analysis and risk assessments at the company level, and approved the business continuity objectives. Additionally, business continuity drills are conducted regularly, and disaster recovery drills are carried out every year for critical information services and systems to verify the effectiveness of relevant procedures and mechanisms.

Supply Chain Risk Management

Given that supply chain cyberattacks have become a potential cybersecurity risk for businesses, Advantech has incorporated information security risks into its supplier evaluation and management mechanisms. Suppliers identified as having significant cybersecurity risks are required to complete a cybersecurity risk self-assessment, which will then be evaluated by the Advantech cybersecurity team to reduce the likelihood of introducing cybersecurity risks through suppliers.

Incident Notification

Advantech has established procedures for reporting and handling cybersecurity incidents. In accordance with the definition and classification of information security incidents, incidents must be reported to IT/OT or relevant departments for processing, with all related records retained. In the event of a significant cybersecurity incident, the severity and scope of the impact will determine whether external parties such as government agencies, customers, or suppliers are notified in compliance with relevant regulations. Additionally, if any cybersecurity vulnerabilities are discovered in the products, ACIRT (Advantech Cybersecurity Incident Response Team) will notify and address the issue with customers.

3.2 IEC 62443 Gaps to CRA Compliance

To clearly illustrate how the IEC 62443 standard addresses the requirements of the Cyber Resilience Act (CRA), the following summary based on Section 4 of the Cyber Resilience Act Requirements Standards Mapping is provided. This summary highlights the relevant sections within the IEC 62443, that correspond to specific CRA requirements.

CRA Requirement	Description	IEC 62443 Part
Coverage of CRA Annex I, Section 1 by IEC 62443		
1	Products designed, developed, and produced with appropriate cybersecurity based on risks	3-2 & 4-1
2	Products delivered without known exploitable vulnerabilities	4-1
3a	Be delivered with a secure by default configuration, including the possibility to reset the product to its original state	GAP
3b	Protection from unauthorized access (authentication, identity, and access management)	4-2
3c	Protection of data confidentiality (encryption at rest and in transit)	4-2
3d	Protection of data integrity (against unauthorized manipulation or modification)	4-2
3e	Process only relevant and necessary data (data minimization)	GAP
3f	Availability of essential functions (resilience against denial-of-service attacks)	4-2

CRA Requirement	Description	IEC 62443 Part
3g	Minimizing negative impact on other services' availability	GAP
3h	Limiting attack surfaces (external interfaces)	4-2
3i	Reduce incident impact using mitigation techniques	3-2
3j	Recording and monitoring of internal activity (security-related information)	4-2
3k	Addressing vulnerabilities through security updates	2-1 & 4-2
Coverage of CRA Annex I, Section 2 by IEC 62443		
1	Manufacturers shall document vulnerabilities and include a software bill of materials	GAP
2	Address and remediate vulnerabilities promptly, including security updates	4-1
3	Regularly test and review product security	GAP
4	Disclose fixed vulnerabilities, including descriptions and remediation info, after updates	4-1
5	Enforce a coordinated vulnerability disclosure policy	GAP
6	Facilitate sharing info on vulnerabilities and provide a contact address for reporting	GAP
7	Provide secure mechanisms for timely updates to fix vulnerabilities	4-1
8	Distribute free security patches promptly with relevant advisories	4-1

The following section lists the remaining requirements from the Cyber Resilience Act (CRA) that are not addressed by the IEC 62443 standard. Each of the following subsections details the unmet requirements and outlines the necessary measures to satisfy them.

Annex I, Section 1, 3a be delivered with a secure by default configuration, including the possibility to reset the product to its original state.
According to the requirements defined in IEC 62443-4-1 SG-3 Security hardening guidelines, a process is employed to create product user documentation that includes guidelines for hardening the product when installing and maintaining the product. It includes descriptions of configurable and default values that include how each affects security along with any potential impact each has on work practices.

According to the requirements defined in IEC 62443-4-2 CR 4.2 Information persistence, components provide the capability to erase all information and ensure that everything is set back to factory settings.

Annex I, Section 1, 3e Process only relevant and necessary data (data minimization)
It's necessary to select secure principles and guidelines as part of the IEC 62443-4-1 process and to establish a well-defined device architecture. An important principle highlighted in the OWASP "Secure Product Design Cheat Sheet" is the Principle of Least Privilege and Separation of Duties. The Principle of Least Privilege is also defined in CCSC3 of IEC 62443-4-2.

Annex I, Section 1, 3g Minimize negative impact on other services' availability.
According to the requirements defined in IEC 62443-4-2 CCSC2 Compensating countermeasures, where there is a need for a great deal of analysis of network security, a secure zone-and-conduit architecture implicitly forces the implementation of a firewall.

According to the requirements defined in IEC 62443-4-2 CR 7.7 Least functionality, components provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.

Advantech incorporates IEC 62443-4-1 SG-3 Security hardening guidelines into above to make components work with secure defaults, which implicitly makes the device independent of other services.

Annex I, Section 2, 1 Manufacturers shall document vulnerabilities and include a software bill of materials.

Advantech implements ongoing monitoring of the cybersecurity status of the entire supply chain to ensure the security of the components used in the products. A comprehensive Software Bill of Materials (SBOM) is created, listing all libraries and external components used in the product's software, along with the version numbers. This SBOM is readily accessible to users and conforms to relevant standards such as ISO/IEC 5921:2021 (SPDX).

Annex I, Section 2, 3 Regularly test and review product security.

Advantech conducts periodic vulnerability assessments, focusing particularly on components that present the highest risk. During the development or maintenance of software components, verification and validation is performed with each new commitment or revision. Risk assessments are re-evaluated whenever there are significant changes due to new threats, vulnerabilities, or a new product release.

Annex I, Section 2, 5 Enforce a coordinated vulnerability disclosure policy.

According to the requirements defined in IEC 62443-4-1 DM-5 Disclosing security-related issues, Advantech informs product users about reportable security-related issues in supported products in a timely manner with content that includes issue description, vulnerability score as per CVSS, affected product version(s) and description of the resolution.

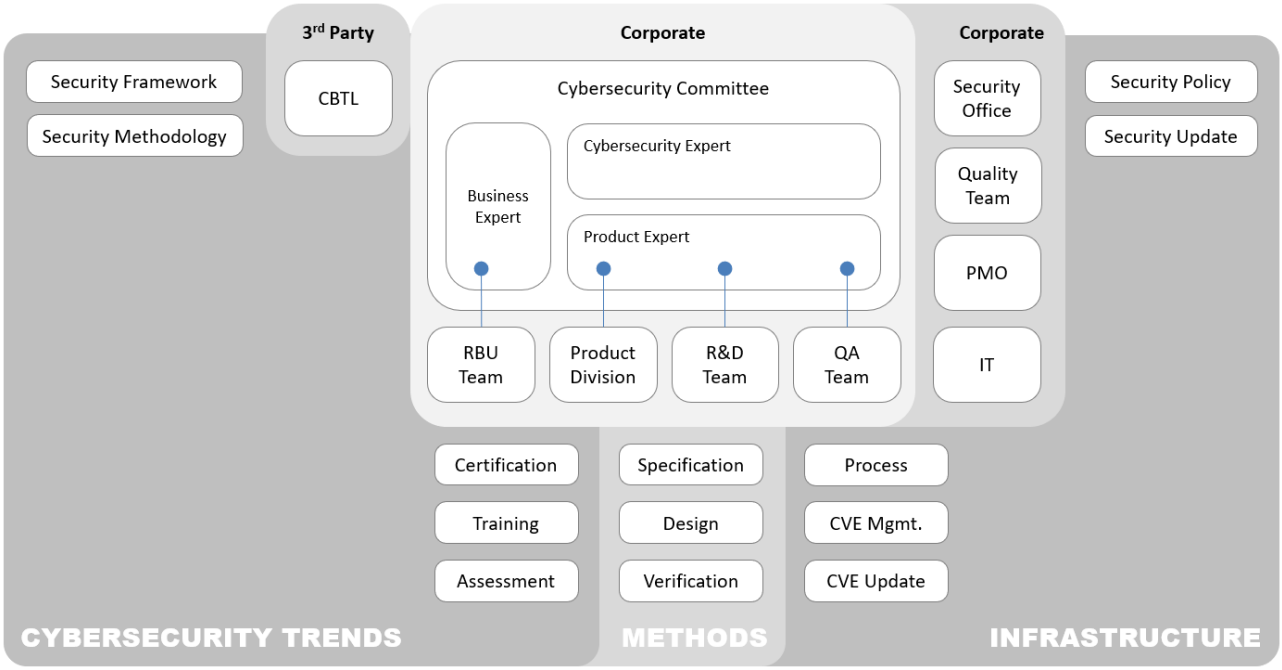
Annex I, Section 2, 6 Facilitate sharing info on vulnerabilities and provide a contact address for reporting.

Advantech implements an incident escalation path and breach notification procedure in the official WEB site. It discloses the security advisory also provide the contact window to report a potential vulnerability by mail to ACIRT@advantech.com.

4 Cybersecurity Governance

4.1 Organizational Structure

For the purpose to enhance security development operation process of Advantech's product or service, the Cybersecurity Committee (CSC) is authorized as the taskforce, with efficient communication and effective management, lead relevant business unit and respondents to achieve the goal for product security development and information security.



Operation responsibility

- Responsible for formulating product security strategy and policy and organizing resources necessary.
- for appointment policy implementation to build the comprehensive security program and ensuring that the processes and results propagated and implemented by secure product development are conforming to the requirements of organization security policy and security regulations.
- Approve the product security development and information security management audit report or work report.
- Responsible for the performance of product security development and related information security management reporting to the first level management.
- Coordinate the cross-departmental matters and responsibility division.
- Responsible for the coordination and discussion of overall security development and information security management.
- Ensure the security development and related information security management activity conforming to the security policy.
- Responsible for the execution, coordination and discussion of other important security developments and related information security management.

4.2 Security Policy

In order to ensure the safe operation of personnel, data, systems, equipment and networks related to information operations of Advantech Co., Ltd. (hereinafter referred to as the company), and to comply with the requirements of relevant laws and regulations, an information security policy (hereinafter referred to as this policy) has been formulated as the highest guiding principle.

Scope

- It is applicable to the security management of the company's information assets, covering its confidentiality, integrity and availability.
- All employees, contractors, consultants, temporary employees, customers, and third-party personnel involved in the company's information operations or data use should follow this policy.

Information Security System and Organization

- Establish an information security organization and specify its rights and responsibilities to promote and maintain related management, execution, and inspection tasks.
- Formulate information security management related methods and procedures to protect the confidentiality, integrity and availability of personnel, data, systems, equipment and networks.
- Convene information security management meetings on a regular basis to review the latest status in internal and external risks, technology and business needs, and take corresponding measures.
- Handle and protect data and system security cautiously in accordance with relevant regulations on information security and personal data protection.

Access Control

- Restrict access to information and information processing facilities.
- Ensure authorized users can access the system and services while preventing unauthorized access.
- Hold users responsible for securing their authentication information.
- System and data usage must be authorized, and access permissions should be granted based on the principle of minimum necessary scope for business needs.

Physical and Environmental Security

- Prevent unauthorized physical access, damage, and interference to organizational information and information processing facilities.
- Prevent loss, damage, theft, or compromise of assets and ensure continuity of organizational operations.

Asset Management

- Identify organizational assets and define appropriate protection responsibilities.
- Ensure all assets are protected at an appropriate level based on their importance to the organization.
- Prevent unauthorized disclosure, modification, removal, or destruction of information stored in the media.

Data Transmission

- Ensure traceability and non-repudiation of data transmission.
- Maintain the reliability and availability of transmission operations.
- Use tamper-evident or tamper-resistant control measures for physical transmission.
- Use prescribed electronic transmission media for data transfer, avoiding the use of illegal or improper transmission media for convenience.
- Do not disclose confidential or sensitive information to other organizations or personnel through any transmission medium, such as data transfer, messaging, speech, or video.
- Internal information websites must grant appropriate access permissions based on authority and job requirements to control access to related documents.

Security Configuration and Handling of Endpoint Devices

- Distribution and retrieval of user endpoint devices.
- Control software installation on user endpoint devices.
- Perform security updates on user endpoint devices.
- Use user endpoint devices through a login process.
- Prevent malware from compromising user endpoint devices.
- Control access to server farms from BYOD (Bring Your Own Device) to prevent BYOD from affecting internal information systems and equipment operations.

Network Security

- Network users can only access network resources within the authorized scope after authorization.
- Appropriate controls should be applied to computer connections using the network system to reduce the risk of unauthorized system access or computer facility compromise.
- The planning of network segmentation should follow the rules of physical separation between internal and external networks, and the use of personal wireless network devices that compromise the security mechanisms of this separation should be prohibited.
- Unauthorized use of wireless networks and private wired equipment to interface with the network is strictly prohibited.

Information Security Incident Management

- Ensure consistent and effective practices for managing information security incidents, including the communication of security events and vulnerabilities.
- Establish response and reporting procedures for information security incidents to enhance the ability of internal personnel to respond to and coordinate in the face of emergencies.

Information System Backup and Redundancy

- Develop backup cycles, methods, and retention periods for information based on availability and integrity requirements and test their effectiveness.
- Protect backup data according to confidentiality requirements to prevent additional security incidents.
- Implement appropriate redundancy and backup mechanisms for information systems and conduct contingency drills to enhance the resilience of information services against threats.

Cryptography

- Implement encryption mechanisms according to regulations, customer requirements, and information asset risk assessments.
- Control operations such as key generation, distribution, activation, storage, update, revocation, archiving, and destruction.

Information Classification and Handling

- Information labeling should cover all formats of information and other related assets.
- Ensure that personnel and other concerned parties are aware of labeling requirements.
- Provide all personnel with necessary awareness methods to ensure correct information labeling and corresponding handling.

Technical Vulnerability Management

- Define and establish roles and responsibilities related to technical vulnerability management.
- Detect vulnerabilities in information assets.
- Manage software update processes to ensure that all authorized software installs the latest approved patches and application updates.
- Use appropriate vulnerability scanning tools for the technology in use to identify vulnerabilities and verify the success of vulnerability remediation.
- Conduct regular information security assessments and audits to evaluate and improve the risk profile of the information environment.

Secure Development Policy

- Ensure that information security is part of the overall information system throughout its entire lifecycle. This also includes requirements for information systems that provide services over public networks.
- When developing new information systems or enhancing the functionality of existing systems, include security requirements in the system functional planning and requirements analysis phase.
- Evaluate security requirements when procuring software.
- The security requirements and controls of the system should be proportional to the value of the information assets and consider the potential damage that insufficient security measures might cause.
- Information systems should protect data to prevent leakage or tampering.

Information Security Policy Review and Maintenance

- This policy should be reviewed at least once a year to reflect the latest developments in relevant laws, technology and the company's business, and be appropriately revised.
- The revision of this policy is approved by the general manager and becomes effective on the announcement day. In addition, interested parties, such as all employees, cooperating manufacturers, suppliers, etc., shall be notified by announcement, writing, e-mail or other methods.
- Consider the confidentiality, integrity, and availability of key systems and important equipment to set information security objectives and regularly measure and review each indicator item at least once a year to ensure the effectiveness of performance.

4.3 Security Infrastructure

Risk Management and Security Measures

Advantech conducts regular risk assessments to identify and mitigate potential cybersecurity threats. Which includes:

- Implement and maintain a risk management process to identify, assess, and manage information security risks.
- Maintain a risk register to document key risk factors, including organizational risk tolerance.
- Have a program to manage risks associated with third-party software, artificial intelligence, and autonomous technologies.

Incident Management

Advantech develops and maintains an incident response plan to manage and mitigate the impact of security incidents. Which includes:

- Implement and maintain a documented cybersecurity incident management program to ensure an organization-wide capability for handling cyber security and privacy related incidents.
- Notify the customer promptly, in accordance with any applicable law or regulation and at any event within 72 hours after discovering any security incidents or threats relating to the Services and/or customer material, data, or information.

Business Continuity and Disaster Recovery

Advantech implements a business continuity plan to ensure the resilience of critical services. The procedures ensure the availability and integrity of data to meet recovery time and point objectives.

Supply Chain

Advantech vets and monitors the suppliers to ensure they meet our stringent security requirements. Include security clauses in contracts with third-party vendors and partners. Implement and maintain a third-party risk management process to effectively oversee and manage risks associated with third-party providers.

Security Awareness & Training

Advantech provides ongoing cybersecurity training for all employees, emphasizing the importance of cybersecurity standard compliance.

4.4 Security Advisory

Advantech maintains a comprehensive vulnerability management process. The security experts rigorously assess potential threats to products and provide timely and transparent advisories to the customers. These advisories offer clear guidance and resources to help mitigate risks and maintain the security of the deployments.

Disclosure of Vulnerabilities

Advantech discloses vulnerabilities of a product as security advisories, which reveals the following information to product users for obtaining a timely update of the software or firmware.

- Affected Products
- Common Vulnerabilities and Exposures (CVE) ID
- CVSS Score
- Reason for Product Change
- Description of the Resolution

Report on Potential Vulnerability

Advantech provides a contact window as ACIRT@advantech.com to report a potential vulnerability, including information such as:

- Affected product and firmware version.
- Description of the vulnerability
- Steps to reproduce vulnerability.

5 Security Management

5.1 IEC 62443-4-1 Certification

The IEC 62443-4-1 specifies the process requirements for the secure development of products used in IACS. It defines secure development life-cycle requirements related to cybersecurity for products intended for use in the industrial automation and control systems environment.

Advantech got certified of IEC 62443-4-1 with Maturity Level 2 in September 2020.

TÜV NORD

Certificate

No. NF1105200005

TUV Asia Pacific Ltd. hereby certifies to the product supplier

Advantech Co., Ltd.
No. 1, Alley 20, Lane 26, Rueiguang Road, Neihu District, Taipei 11491, Taiwan

that the product development lifecycle
meets the process requirements listed in the below mentioned standard(s)

- IEC 62443-4-1:2018
  SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS
  PART 4-1: Secure product development lifecycle requirements
  Maturity Level 2: Managed

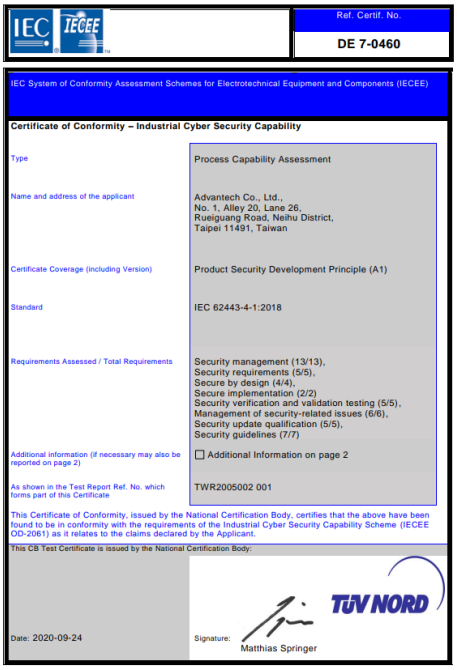
Base of certification is the report
TWR2005002 001 in the valid version.

Valid until: 2025-09-24

Taipei, 2020-09-25

Certification Department
TUV Asia Pacific Ltd.

The certificate can be verified by info.pc@tuv-nord.com The certification system is based on ISO 17065.
Report of voluntary examinations of the subject(s) is for compliance with the requirements, where the standard(s) is accordingly applied. It is confirmed that the applicant has chosen to address the CyberSecurity via compliance with the standard(s) listed in this report.The certificate must be associated with report.



IEC IECEE

Ref. Certif. No.
DE 7-0460

IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)

Certificate of Conformity – Industrial Cyber Security Capability

Type	Process Capability Assessment
Name and address of the applicant	Advantech Co., Ltd., No. 1, Alley 20, Lane 26, Rueiguang Road, Neihu District, Taipei 11491, Taiwan
Certificate Coverage (including Version)	Product Security Development Principle (A1)
Standard	IEC 62443-4-1:2018
Requirements Assessed / Total Requirements	Security management (13/13), Security requirements (5/5), Secure by design (4/4), Secure implementation (2/2) Security verification and validation testing (5/5), Management of security-related issues (6/6), Security update qualification (5/5), Security guidelines (7/7)
Additional information (if necessary may also be reported on page 2)	☐ Additional Information on page 2
As shown in the Test Report Ref. No. which forms part of this Certificate	TWR2005002 001

This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.

This CB Test Certificate is issued by the National Certification Body:

Date: 2020-09-24

Signature: Matthias Springer

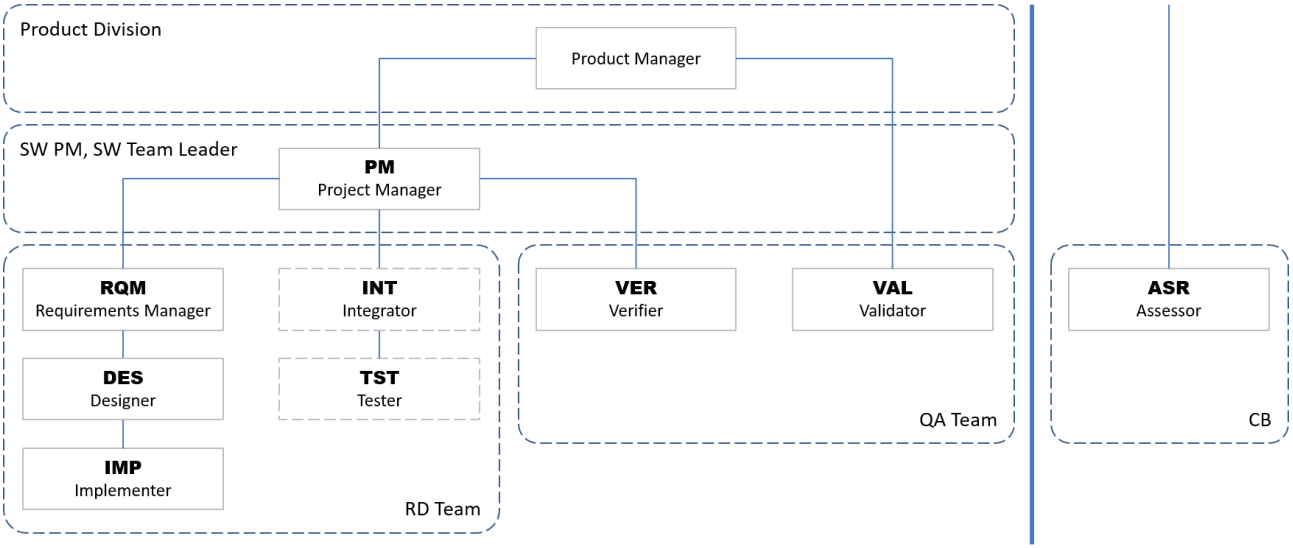
TÜV NORD

5.2 Secure Software Development Life Cycle (SSDLC)

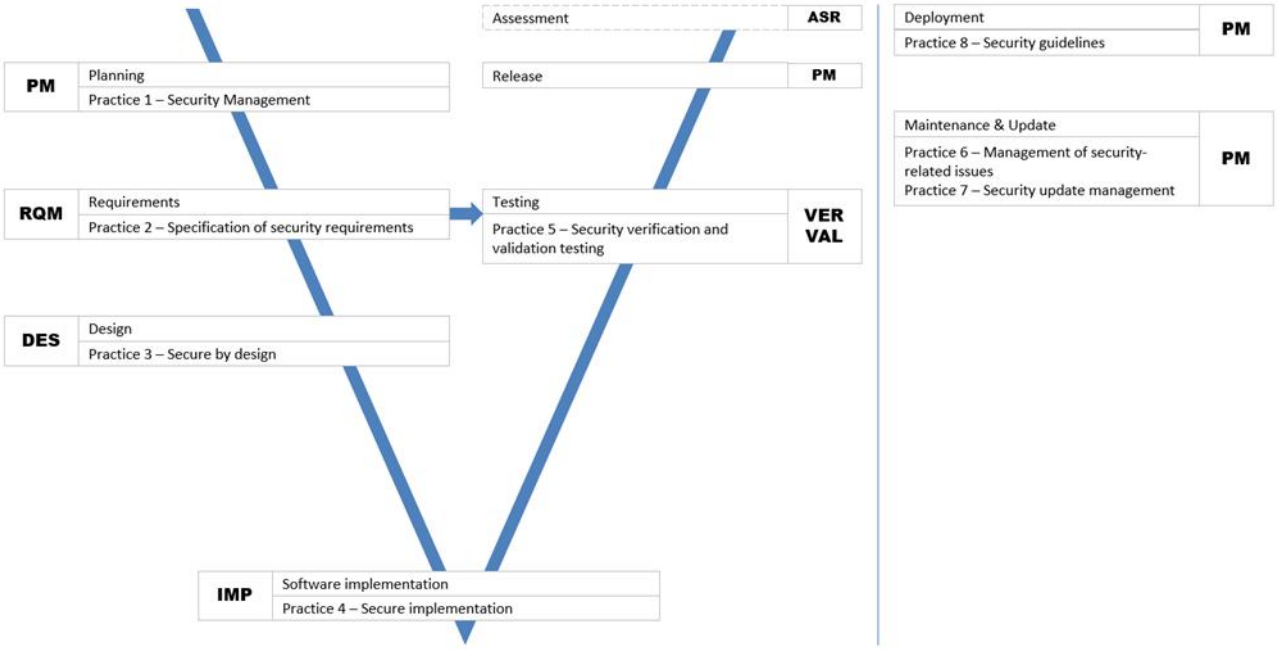
According to requirements defined in IEC 62443-4-1 Practice 1 SM-1 Development Process, Advantech established the Secure Software Development Life Cycle (SSDLC) with V-model.

This V-model illustrates the IEC 62443-4-1 interpretation of the Secure Software Development Life Cycle (SSDLC). This proactive approach integrates security related best practices into the traditional Software Development Life Cycle (SDLC) that will be familiar to developers in the functional safety domain. It shows how the use of automated and integrated tools can help to achieve compliance. Verification and validation play an important role in the process, and several testing techniques are applicable to the standard's recommended requirement-based testing approach.

Preferred Organizational Structure for SSDLC



SSDLC with V-Model



Planning

According to requirements defined in IEC 62443-4-1 Practice 1 – Security Management, Advantech ensures a general product development/maintenance/support process is documented and enforced that is consistent and integrated with commonly accepted product development processes.

The following processes should be defined and executed in the planning stage.

- Role & Responsibilities
- Product Applicability
- File Integrity
- Development Environment Security
- Key Management
- 3rd-party Component Management

Requirements

According to requirements defined in IEC 62443-4-1 Practice 2 – Security Requirements, Advantech ensures that security requirements include the following information:

- Security Context
- Thread Model
- Product Security Requirements Content in a Software Requirements Specification (SRS)

This information is referred by VER/VAL for preparation of verification and validation in testing stage.

Design

According to requirements defined in IEC 62443-4-1 Practice 3 – Secure by Design, Advantech ensures a secure design that identifies and characterizes each interface of the product, including physical and logical interfaces, is developed and documented. It implements multiple layers of defense using a risk-based approach based on the threat model; conducts design reviews to identify, characterize and track to closure security-related issues associated with each significant revision of the secure design; and ensures that secure design best practices are documented and applied in this stage.

Software Implementation

According to requirements defined in IEC 62443-4-1 Practice 4 – Secure Implementation, Advantech incorporates security coding standards that are periodically reviewed and updated; ensures that implementation reviews are performed for identifying, characterizing and tracking to closure security-related issues associated with the implementation.

Testing

According to requirements defined in IEC 62443-4-1 Practice 5 – Security Verification and Validation Testing, Advantech performs security requirements testing and threat mitigation testing on the products; vulnerability testing and penetration testing will be performed by 3rd party test lab.

Release

According to requirements defined in IEC 62443-4-1 Practice 6 – Management of Security-related Issues, Advantech ensures that reported security-related issues are reviewed, assessed, addressed and disclosed before the software or firmware is released.

Deployment

According to requirements defined in IEC 62443-4-1 Practice 8 – Security Guidelines, Advantech creates product user documentation that includes guidelines for hardening the product when installing and maintaining the product, until removing the product from use.

This document represents responsibilities and actions necessary for users, including administrators, to securely operate the product; and assumptions regarding the behavior of the user/administrator and their relationship to the secure operation of the product. The following recommendations are necessarily described in this document.

- User account permissions (access control) and privileges (user rights) needed to use the product.
- Default accounts used by the product and instructions for changing default account names and passwords.

Maintenance & Update

According to requirements defined in IEC 62443-4-1 Practice 7 – Security Update Management, Advantech ensures that security updates for all supported products and product versions are made available to product users in a manner that facilitates verification that the security patch is authentic.

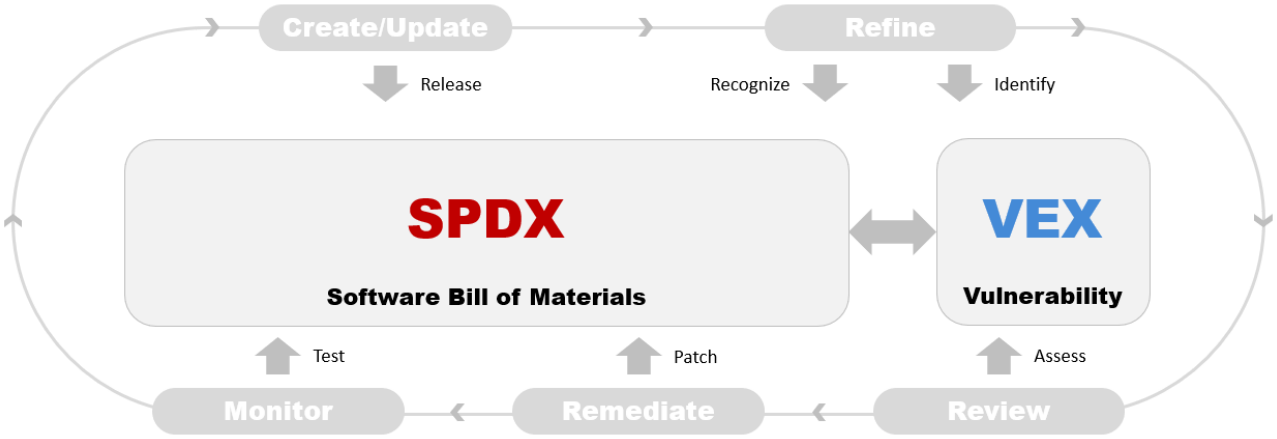
Assessment

Cybersecurity compliance assessment is performed by outside assessors to ensure independence.

5.3 Soft Bill of Material (SBOM)

According to the requirements defined in IEC 62443-4-1 Practice 7 – Security Update Management, Advantech established a SBOM management mechanism to create/refine/review/remediate/monitor and update third-party software components with security patches.

An SBOM is a document that tracks the supply chain in software development. It keeps track of every third-party library, script, CI/CD application, artifact (e.g., Docker), license, and version integrated into your applications. For small businesses with just one application, it might seem like tracking the supply chain is simple, but it can soon become overwhelming as your software development lifecycle adds several more moving parts. An SBOM ensures that every element integrated into your software including dependencies are tracked and can be audited for security issues.



Create/Update
Collect the SBOM parts from multiple sources in a wide range of formats from across the software supply chain. This stage makes a delivery of a single, unified SBOM with a commonly accepted format. It expands the level of transparency into your applications beyond just the code you control.

Refine
Organize and refine all these SBOM parts. This stage makes a reorganization of SBOM parts to present the necessary information as well as identification of its relevant vulnerabilities from the source of vendor or open database.

Review
Perform a comprehensive review on vulnerabilities and assess the potential risk. This stage makes an identification of root causes and attack manners digging the vulnerabilities out.

Remediate

Manage remediation work to address security vulnerability, license compliance, and operational risk issues. This stage makes a patch or mitigation plan to the SBOM.

Monitor

Continuously monitor the risks across the portfolio of software applications and the supply chain.

System Package Data Exchange (SPDX)

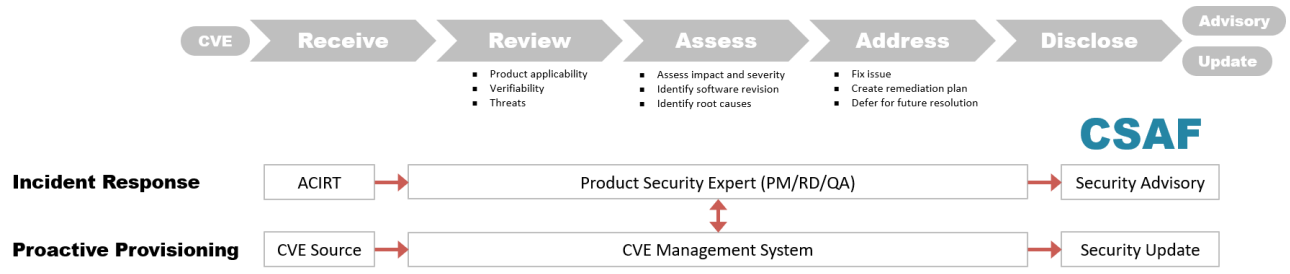
SPDX is an open standard capable of representing systems with digital components as bills of materials (BOMs).

Vulnerability Exploitability eXchange (VEX)

VEX is a standardized format used to convey information about the exploitability of vulnerabilities in software products.

5.4 Vulnerability Management

According to the requirements defined in IEC 62443-4-1 Practice 6 – Management of Security-related Issues, Advantech established a vulnerability management mechanism to gather/review/assess/address and disclose vulnerability/CVE based on SBOM or open-source list of the product.



For incident response, Advantech Cybersecurity Incident Response Team (ACIRT) receives the vulnerabilities from customers. The product security experts, including the product manager, development team and quality assurance team start to review/assess/address these issues until the threats are mitigated. A security advisory is published to disclose which manner or countermeasure is made for reducing the risk of vulnerabilities.

In an advanced process of proactive provisioning, Advantech monitor vulnerabilities from CVE database (https://www.cvedetails.com/) and synchronize to customers proactively. The product security expert performs a monthly review/update and report to customers in each 6 months. If the incident or vulnerability is critical, Advantech timely notifies the customers and comes out an update software/firmware.

Receive

According to the requirements defined in IEC 62443-4-1 DM-1 Receiving notifications of security-related issues, Advantech receives and tracks to closure security-related issues in the product reported by internal and external sources including testers, 3rd party component suppliers, product developers and product users.

Review

According to the requirements defined in IEC 62443-4-1 DM-2 Reviewing security-related issues, Advantech ensures that reported security-related issues are investigated in a timely manner to determine their applicability, verifiability and threats that trigger the issue.

The timeliness is driven by market forces.

Assess

According to the requirements defined in IEC 62443-4-1 DM-3 Assessing security-related issues, Advantech analyzes security-related issues to assess the impact with security context, defense in depth strategy of the product. The root causes and related security issues are identified with methodical approaches.

Address

According to the requirements defined in IEC 62443-4-1 DM-4 Addressing security-related issues, Advantech addresses security-related issues and determines whether to report them based on the results of the impact assessment. It establishes an acceptable level of residual risk that is applied when determining an appropriate way to address each issue.

Advantech reviews open security-related issues periodically to ensure that issues are being addressed appropriately.

Disclose

According to the requirements defined in IEC 62443-4-1 DM-5 Disclosing security-related issues, Advantech informs product users about reportable security-related issues in supported products in a timely manner with content that includes issue description, vulnerability score as per CVSS, affected product version(s) and description of the resolution.

Common Security Advisory Framework (CSAF)

CSAF is a language exchange for Security Advisories. It plays a crucial role in the cybersecurity arena since it allows stakeholders to automate the creation and consumption of security vulnerability information and remediation.

Advantech presents the security advisories as a unified machine-readable format defined by CSAF.

6 Secure Product

6.1 IEC 62443-4-2 Compliance

With the rapid growth of IoT and edge computing, managing and operating computing devices has become increasingly complex. The IEC 62443 series of standards provide a comprehensive security framework for IoT, widely adopted across industries such as energy, healthcare, and transportation, to prevent losses from information security vulnerabilities. However, the framework can be difficult to navigate. IEC 62443-4-2 focuses on security specifications for systems, components, and more, focusing on protection at the lower embedded level. For equipment builders or system integrators, understanding and implementing these standards can be challenging.

Advantech offers a comprehensive solution to enhance software protection and significantly improve the efficiency of testing and certification. Advantech joins forces with Bureau Veritas, a global leader in testing, inspection, and certification, to help customers overcome security challenges in AIoT and edge computing.

For IEC 62443-4-2 functional security, Advantech's x86-based products will gradually incorporate basic protection measures, including firmware, operating systems, IoT connections, and more. These products will utilize tools such as the Trusted Platform Module (TPM) and a whitelist control to enhance overall system security.

For advanced testing and certification services, Advantech offers Verification of Conformity (VoC) or formal certification (CB). Customers can choose depending on the need for IEC 62443-4-2 compliance. With their existing functional security testing process methods, Advantech can help customers significantly reduce both the time and costs associated with certification.

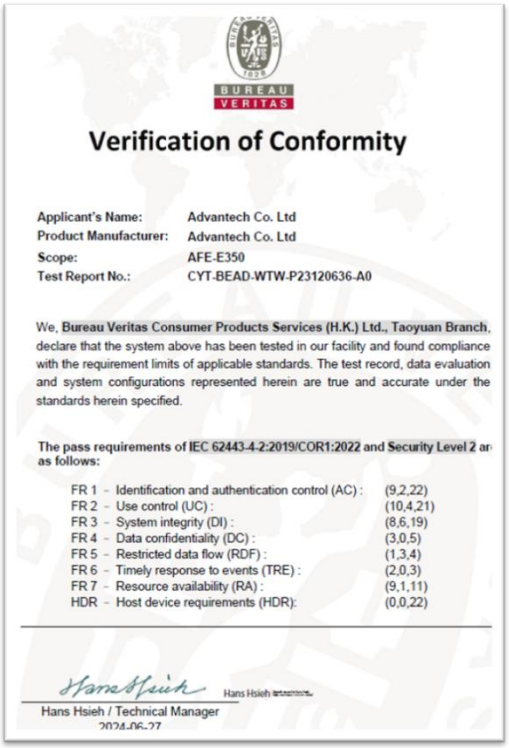
Review of IEC 62443-4-1 Best Practice	Verification of Conformity (VoC)	Formal certification (CB)
Product security context	○	●
Threat model	○	●
Product security requirements	●	●
Security Requirements Testing	●	●
Threat Mitigation Testing		●
Vulnerability Analysis (VA)		●
Penetration Testing (PT)		●
Security Guideline		●

● Fully performed.

○ Partial performed due to the edge computing platforms cooperating with customer's software applications. The security context and threat model are defined when these software applications are installed. It should be fully performed on a software application-available device.

Example of Verification of Conformity (VoC)

Advantech Application Focus Embedded Solutions, 2024-8-2, Bureau Veritas



BUREAU VERITAS

Verification of Conformity

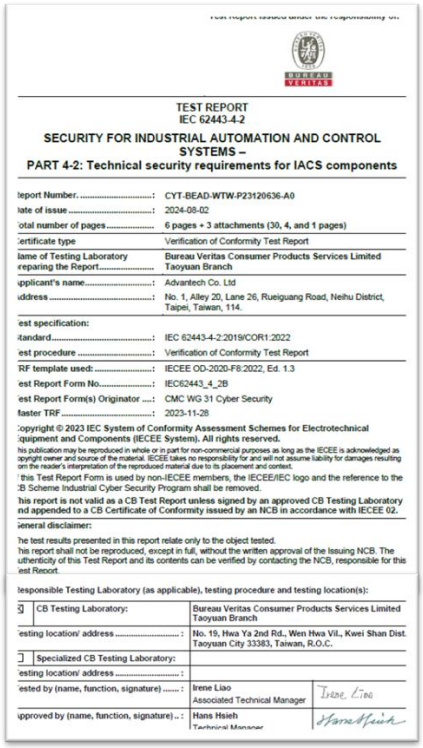
Applicant's Name: Advantech Co. Ltd
Product Manufacturer: Advantech Co. Ltd
Scope: AFE-E350
Test Report No.: CYT-BEAD-WTW-P23120636-A0

We, **Bureau Veritas Consumer Products Services (H.K.) Ltd., Taoyuan Branch**, declare that the system above has been tested in our facility and found compliance with the requirement limits of applicable standards. The test record, data evaluation and system configurations represented herein are true and accurate under the standards herein specified.

The pass requirements of IEC 62443-4-2:2019/COR1:2022 and Security Level 2 ar as follows:

FR 1	Identification and authentication control (AC) :	(9,2,22)
FR 2	Use control (UC) :	(10,4,21)
FR 3	System integrity (DI) :	(8,6,19)
FR 4	Data confidentiality (DC) :	(3,0,5)
FR 5	Restricted data flow (RDF) :	(1,3,4)
FR 6	Timely response to events (TRE) :	(2,0,3)
FR 7	Resource availability (RA) :	(9,1,11)
HDR	Host device requirements (HDR):	(0,0,22)

Hans Hsieh / Technical Manager
2024-06-27



TEST REPORT
IEC 62443-4-2
SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –
PART 4-2: Technical security requirements for IACS components

eport Number.	CYT-BEAD-WTW-P23120636-A0
ate of issue	2024-08-02
otal number of pages	6 pages + 3 attachments (30, 4, and 1 pages)
ertificate type	Verification of Conformity Test Report
ame of Testing Laboratory reparing the Report	Bureau Veritas Consumer Products Services Limited Taoyuan Branch
pplicant's name	Advantech Co. Ltd
ddress	No. 1, Alley 20, Lane 26, Rueiguang Road, Neihu District, Taipei, Taiwan, 114.
est specification:	
tandard	IEC 62443-4-2:2019/COR1:2022
est procedure	Verification of Conformity Test Report
RF template used:	IECEE OD-2020-F8:2022, Ed. 1.3
est Report Form No.	IEC62443_4_2B
est Report Form(s) Originator	CMC WG 31 Cyber Security
laster TRF	2023-11-28

opyright © 2023 IEC System of Conformity Assessment Schemes for Electrotechnical quipment and Components (IECEE System). All rights reserved.
his publication may be reproduced in whole or in part for non-commercial purposes as long as the IECEE is acknowledged as opyright owner and source of the material. IECEE takes no responsibility for and will not assume liability for damages resulting om the reader's interpretation of the reproduced material due to its placement and context.
his Test Report Form is used by non-IECEE members, the IECEE/IEC logo and the reference to the B Scheme Industrial Cyber Security Program shall be removed.
his report is not valid as a CB Test Report unless signed by an approved CB Testing Laboratory nd appended to a CB Certificate of Conformity issued by an NCB in accordance with IECEE 02.
eneral disclaimer:
he test results presented in this report relate only to the object tested.
his report shall not be reproduced, except in full, without the written approval of the Issuing NCB. The uthenticity of this Test Report and its contents can be verified by contacting the NCB, responsible for this est Report.

esponsible Testing Laboratory (as applicable), testing procedure and testing location(s):

☒	CB Testing Laboratory:	Bureau Veritas Consumer Products Services Limited Taoyuan Branch
	esting location/ address	No. 19, Hwa Ya 2nd Rd., Wen Hwa Vil., Kwei Shan Dist. Taoyuan City 33383, Taiwan, R.O.C.
☐	Specialized CB Testing Laboratory:	
	esting location/ address	
	ested by (name, function, signature)	Irene Liao Associated Technical Manager
	pproved by (name, function, signature)	Hans Hsieh Technical Manager

Example of Formal certification (CB)

Advantech Industrial Ethernet Switch, 2021-11-22, TUV NORD

TÜV NORD

Certificate

No. NF1105210008

TUV Asia Pacific Ltd. hereby certifies to the product supplier

Advantech Co., Ltd.
No. 1, Alley 20, Lane 26, Rueiguang Road, Neihu District, Taipei 11491, Taiwan

that Industrial Ethernet Switch; EKI-77**XX** Series, EKI-74**XX** Series
meets the product capability requirements listed in the below mentioned standard(s)

- IEC 62443-4-1:2018
  SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS
  PART 4-1: Secure product development lifecycle requirements
  Maturity Level 2
- IEC 62443-4-2:2019
  SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS
  PART 4-2: Technical security requirements for IACS components
  Security Level 2

Base of certification is the report
TWR2108009 001 and TWR2108009 002 in the valid version.

Valid until: 2026-11-24

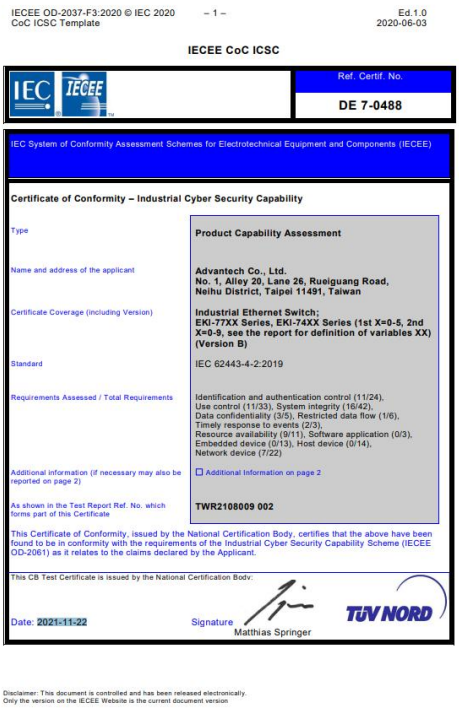
Taipei, 2021-11-23

Certification Department
TUV Asia Pacific Ltd.

TÜV NORD Certified Product

TAF Product Certification PC 029

The certificate can be verified by info.pc@tuv-nord.com TAF ISO 17065 accredited no. PC029 for certification.
Report of voluntary examinations of the subject(s) is for compliance with the requirements, where the standard(s) is accordingly applied. It is confirmed that the applicant has chosen to address the CyberSecurity via compliance with the standard(s) listed in this report.The certificate must be associated with report.



IECEE OD-2037-F3:2020 © IEC 2020 – 1 – Ed.1.0
CoC ICSC Template 2020-06-03

IECEE CoC ICSC

IEC IECEE

Ref. Certif. No.
DE 7-0488

IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)

Certificate of Conformity – Industrial Cyber Security Capability

Type	**Product Capability Assessment**
Name and address of the applicant	**Advantech Co., Ltd.** **No. 1, Alley 20, Lane 26, Rueiguang Road,** **Neihu District, Taipei 11491, Taiwan**
Certificate Coverage (including Version)	**Industrial Ethernet Switch;** **EKI-77XX Series, EKI-74XX Series (1st X=0-5, 2nd X=0-9, see the report for definition of variables XX)** **(Version B)**
Standard	IEC 62443-4-2:2019
Requirements Assessed / Total Requirements	Identification and authentication control (11/24), Use control (11/33), System integrity (16/42), Data confidentiality (3/5), Restricted data flow (1/6), Timely response to events (2/3), Resource availability (9/11), Software application (0/3), Embedded device (0/13), Host device (0/14), Network device (7/22)
Additional information (if necessary may also be reported on page 2)	☐ Additional Information on page 2
As shown in the Test Report Ref. No. which forms part of this Certificate	**TWR2108009 002**

This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.

This CB Test Certificate is issued by the National Certification Body:

Date: 2021-11-22 Signature Matthias Springer

TÜV NORD

Disclaimer: This document is controlled and has been released electronically.
Only the version on the IECEE Website is the current document version

6.2 IEC 62443 Certification Solution

Advantech's IEC62443-4-2 certification solution offers a comprehensive one for organizations seeking to meet the cybersecurity standards outlined in the IEC 62443 series, specifically the IEC62443-4-2 standard, which is crucial for ensuring the security of industrial automation and control systems. By leveraging deep expertise gained from BV (NCB) training, Advantech helps streamline the certification process, significantly reducing both the time and cost typically associated with obtaining official IEC62443-4-2 certification.

The solution involves meticulous preparation of pre-compliant IEC62443-4-2 reports that are reviewed by BV to expedite certification approval, ensuring compliance with critical cybersecurity requirements. Advantech's approach covers both hardware and software aspects, aligning with the best practices for secure system design. This includes configuring secure operating system environments such as Windows and Ubuntu, with built-in security measures like Trellix whitelisting, BitLocker encryption, Acronis backup solutions, and BIOS-level security protections, including TPM 2.0 for enhanced data encryption.

The hardware security measures also include protective mechanisms such as secure boot, BIOS-level safeguards against cross-flashing, and specialized physical hardware protection, such as tamper-evident seals and case locks, to prevent unauthorized access or modification. Additionally, Advantech ensures that all systems meet the highest standards for secure communication, with protocols such as TLS 1.2 and 1.3, and essential safeguards for software integrity, including trusted firmware updates and the use of cryptographic techniques to validate software authenticity.

With this solution, Advantech not only positions organizations to meet IEC62443-4-2 certification requirements but also enhances their overall security posture, enabling them to comply with other specialized certifications like SEMI-E187 for semiconductor industries, IEC 80001 for healthcare applications, or aim at Smart Energy. Last but not least, Advantech enables organizations to remain compliant with various regulatory requirements, such as those under CRA (Cyber Resilience Act); RED-DA (Radio Equipment Directive Delegated Act), ensuring secure and efficient operations across industries. Let's have a look at Advantech's efforts and technological evolution in this area.

Deep Research
- Studying IEC 62443-4-2's security controls and their applicability to your product and industry.
- Build a team with strong cybersecurity capabilities and expertise.

Function Spec Mapping
- Translating the product's technical specifications into actionable security requirements.
- Identifying Security Needs and Gap Analysis

Initial Test Case
- Defining and developing security test cases that validate compliance with the standard.
- Thoroughly documenting to track performance and identify any areas of concern.

Obey Product Safety Process
- Products are developed in accordance with the IEC 62443-4-1 development process and fulfill the functional security requirements of 4-2.

Audited by Bureau veritas
- BV's security experts perform on-site strict inspection such BIOS security features, and OS security configurations.
- Advantech continuously fix flaws to achieve compliance

Iteratively Optimize
- Updating test cases and improving security measures as new vulnerabilities are identified or as the standard evolves.

By streamlining the certification process, Advantech helps reduce the complexity and overhead of compliance, allowing organizations to focus more on their core operations while ensuring their systems are robust, secure, and prepared for future certifications.

Review of IEC 62443-4-1 Best Practice	Verification of Conformity (VoC)	Formal certification (CB)
Product security context	○	●
Threat model	○	●
Product security requirements	●	●
Security Requirements Testing	●	●
Threat Mitigation Testing		●
Vulnerability Analysis (VA)		●
Penetration Testing (PT)		●
Security Guideline	●	●

● Fully performed.

○ Partial performed due to the edge computing platforms cooperating with customer's software applications. The security context and threat model are defined when these software applications are installed. It should be fully performed on a software application-available device.

6.3 Security Requirements

Advantech made product security features and specifications based on the requirements of IEC 62443-4-2. The following mapping presents all fundamental requirements defined in IEC 62443-4-2 to corresponding methods.

IEC 62443-4-2 Fundamental Requirement	Cybersecurity Methodology
FR 1 Identification and authentication control	Identification, Authentication
FR 2 Use control	Authorization, Least Privilege, Accounting, Access Control
FR 3 System integrity	Secure Boot, Digital Signature Verification, Integrity Checks
FR 4 Data confidentiality	Encryption, Data Privacy Controls
FR 5 Restricted data flow	Network Segmentation, Conduit Protection
FR 6 Timely response to events	Auditing, Monitoring, Incident Response, Event Logging
FR 7 Resource availability	DoS Protection, Redundancy, Backup & Recovery

These methods are summarized as the AAA model and CIA triad, the well-known cybersecurity methodologies to be employed on products.

AAA Model

The objectives of cybersecurity are realized using the AAA or triple-A model. The first A refers to Authentication, which is the process of proving that you are who you say you are. When you claim to be someone, that is called identification; but when you prove it, that is authentication. Authentication requires proof in one of three possible forms: something you know, like a password; something you have, like a key; something you are, like fingerprint. The combination of more than one of these categories is called multifactor authentication.

The second A in the AAA model is Authorization. Authorization means providing the correct level of access that a user should have based on their credentials. This is tied to the principle of least privilege, which states that users, devices, programs and processes should be granted enough permission to do their required functions.

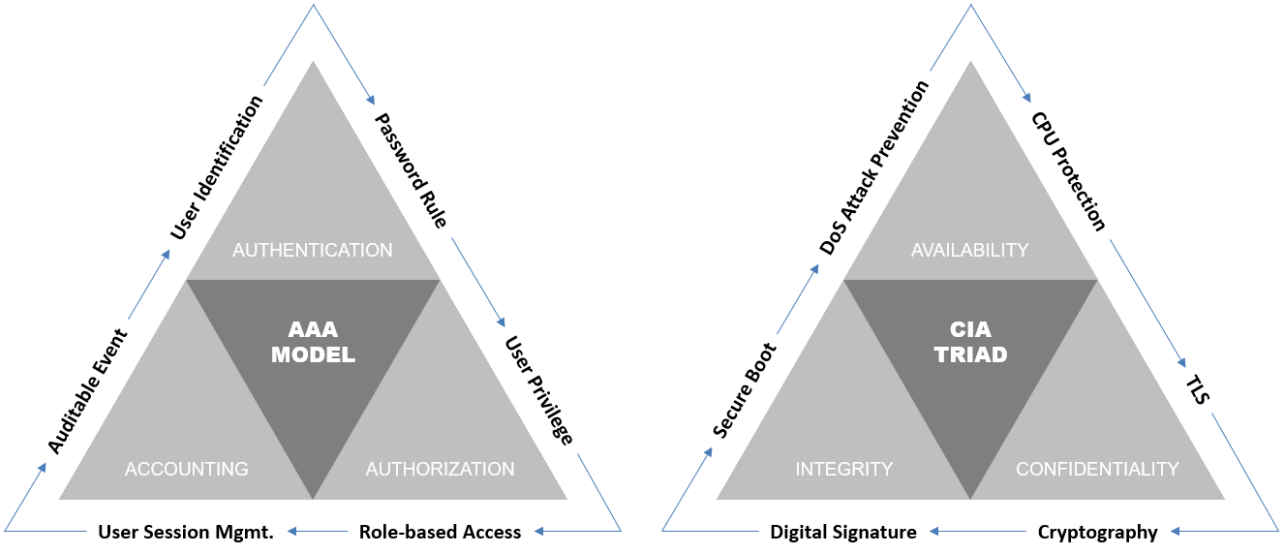
The last A in the AAA model is accounting, which is keeping track of what users do while they are logged into a system. From a forensics perspective, tracing back to events leading up to a cybersecurity incident can prove the non-repudiation to an investigation.

CIA Triad

The CIA triad describes the three important goals of cybersecurity. The C stands for confidentiality. Cybersecurity requires privacy in data and information. Certain people, devices, or processes should be permitted or restricted from seeing data and files. Confidentiality is concerned with viewing of data or information because if the wrong people see data or information they are not authorized, many problems could arise.

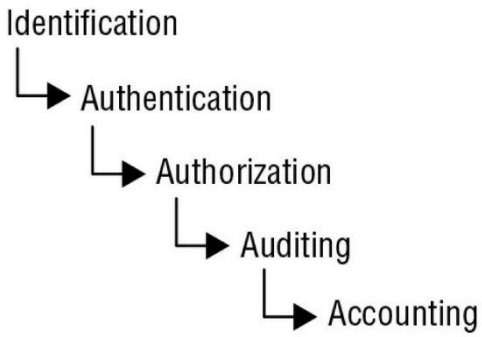
The I in the CIA model stands for integrity. Cybersecurity requires us to feel safe that data transmitted, processed, and stored has not been changed from its original form either accidentally or maliciously.

For the last letter A, it stands for availability. Availability guarantees that with all the cybersecurity measures in place for dealing with hardware, software, people, processes and more, users who are authorized to do their job should be able to do so. It requires that authorized users should be able to access the resources they need to do their job with easy while ensuring that the system has full tolerance and load balancing in the event of cybersecurity incident or disaster.



6.4 Authentication, Authorization and Accounting (AAA)

AAA is a framework used to manage user access, enforce user policies and privileges, and measure the consumption of network resources. Authentication is concerned with proving identity, authorization with granting permissions, accounting with maintaining a continuous and robust audit trail via logging.



Identification

Claiming to be an identity when attempting to access a secure area or system.

According to requirements defined in IEC 62443-4-2 CR 1.1 Human user identification and authentication, components provide the capability to identify all human users on all interfaces capable of human user access.

According to requirements defined in IEC 62443-4-2 CR 1.4 Identifier management, components provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly.

Authentication
Proving that you are that identity.

According to requirements defined in IEC 62443-4-2 CR 1.1 Human user identification and authentication, components provide the capability to authenticate all human users on all interfaces capable of human user access.

According to requirements defined in IEC 62443-4-2 CR 1.5 Authenticator management, components provide the capability to:

- support the use of initial authenticator content.
- support the recognition of changes to default authenticators made at installation time.
- function properly with periodic authenticator change/refresh operation; and
- protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.

Authorization
Defining the permissions (i.e., allow/grant and/or deny) of a resource and object access for a specific identity.

According to requirements defined in IEC 62443-4-2 CR 2.1 Authorization enforcement, components provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.

Auditing
Recording a log of the events and activities related to the system and subjects.

According to requirements defined in IEC 62443-4-2 CR 2.8 Auditable events, components provide the capability to generate audit records relevant to security for the following categories:

- access control
- request errors
- control system events
- backup and restore event
- configuration changes
- audit log events

Accounting
Reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions.

According to requirements defined in IEC 62443-4-2 CR 2.12 Non-repudiation, components provide the capability to determine whether a given human user took a particular action.

6.5 Confidentiality

Information Confidentiality
According to requirements defined in IEC 62443-4-2 CR 4.1 Information confidentiality, components provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported and support the protection of the confidentiality of information in transit.

In general, the password of each account is defined as sensitive information. Advantech provides passwords encrypted and stored in configuration to protect confidentiality.

In the process of user authentication and authorization, username and password are exchanged between client and server via protocols. To protect the confidentiality of account information in transit, Advantech utilizes HTTPS or SSH which frame encryption is performed.

Use of Cryptography
According to requirements defined in IEC 62443-4-2 CR 4.3 Use of cryptography, components use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations. Advantech utilizes Transport Layer Security (TLS) to replace outmoded Secure Socket Layer (SSL) to carry out application layer security such as HTTPS and SSH.

Currently Advantech uses TLS 1.2 or higher version to implement cryptographic security mechanisms.

6.6 Integrity

Communication Integrity
According to requirements defined in IEC 62443-4-2 CR 3.1 Communication integrity, components provide the capability to protect integrity of transmitted information. For the requirement with a higher security level, component is capable to verify the authenticity of received information during communication.

In general, HTTPS and SSH are implemented over Transport Layer Security (TLS) to ensure integrity and authenticity in communication.

Information integrity

According to requirements defined in IEC 62443-4-2 CR 3.4 Software and information integrity, components provide the capability to perform or support integrity and authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks.

It utilizes the digital signature technology to attach in software/firmware/configuration. The digit signature from Advantech computes the hash of software/firmware/configuration then encrypt. This mechanism is used to check the integrity and authenticity at the same time before software/firmware/configuration are applied to components. In other words, it checks the integrity and authenticity in the software/firmware/configuration update stage of this component.

Session integrity

According to requirements defined in IEC 62443-4-2 CR 3.8 Session integrity, components provide mechanisms to protect the integrity of communications sessions. It includes:

- Invalidate session identifiers upon user logout or other session termination.
- Generate a unique session identifier for each session and recognize only session identifiers that are system-generated.
- Generate unique session identifiers with commonly accepted sources of randomness.

Physical Integrity

According to requirements defined in IEC 62443-4-2 CR 3.11 Physical tamper resistance and detection, components provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

Advantech provides physical tamper resistance with Anti-theft Screw and tamper detection with Warranty Seal.

Roots of Trust Integrity

According to requirements defined in IEC 62443-4-2 CR 3.12 Provisioning product supplier roots of trust and CR 3.13 Provisioning asset owner roots of trust, components provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier/asset owner keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

Boot Process Integrity

According to requirements defined in IEC 62443-4-2 CR 3.14 Integrity of the boot process, component verifies the integrity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.

Advantech implements secure boot mechanisms by provisioning the public key (roots of trust) and using of the commonly accepted cryptography.

6.7 Availability

Denial of Service Prevention

According to requirements defined in IEC 62443-4-2 CR 7.1 Denial of service protection, components provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.

According to requirements defined in IEC 62443-4-2 CCSC 1 Support of essential functions, Advantech defines the essential functions and security context for each product. To avoid the resource exhaust by a DoS event, the limited resource allocation is made when the DoS events are detected. Advantech launches degraded mode on each product, which keeps all essential services alive in a DoS attack or flooding storm.

Control System Backup/Recovery/Reconstitution

According to requirements defined in IEC 62443-4-2 CR 7.3 Control system backup, components provide the capability to participate in system level backup operations in order to safeguard the component state. The backup process shall not affect the normal component operations. According to requirements defined in IEC 62443-4-2 CR 7.4 Control system recovery and reconstitution, components provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.

Advantech provides the software/firmware/configuration backup and restore to keep the component state which user and system level information are included. When the backup is performed, the digital signature is attached. This makes software/firmware/configuration not changeable due to the digit signature including a content hash to prevent the tampering.

Least Functionality

According to requirements defined in IEC 62443-4-2 CR 7.7 Least functionality, components provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.

Advantech defines the necessary functions based on CCSC 1 and specifically restricts the use of unnecessary functions, ports, protocols and/or services as follows.

L4 Protocol	L4 Port	Service	Default Configuration
TCP	22	SSH	Enabled
	23	TELNET	Disabled
	80	HTTP	Disabled
	443	HTTPS	Enabled
UDP	67	DHCP	Disabled
	123	NTP	Disabled

Component Inventory

According to requirements defined in IEC 62443-4-2 CR 7.8 Control system component inventory, components provide the capability to support a control system component inventory with a product/model name and software/hardware revision.

Advantech provides an accessible interface to disclose the necessary information been integrated into a control system for inventory management by system integrators. The information includes identification of the component and corresponding hardware/software revision to be recorded in database for a system level continuous monitoring.

6.8 Verification & Validation

Vulnerability Analysis (VA)

According to requirements defined in IEC 62443-4-1 SVV-3 Vulnerability testing, a process is employed for performing tests that focus on identifying and characterizing potential security vulnerabilities in the product. The testing includes:

- Fuzzing Testing
- Attack Surface Analysis for weak access control list, exposed ports and services running with elevated privileges
- Black Box Testing
- Binary Scan

To consider the high cost and effort of obtaining an authoritative VA tool, Advantech entrusts 3rd party CB testing laboratories (CBTLs) to perform the vulnerability analysis.

Penetration Testing (PT)

According to requirements defined in IEC 62443-4-1 SVV-4 Penetration testing, a process is employed to identify and characterize security-related issues via tests that focus on discovering and exploiting security vulnerabilities in the product.

To consider the expertise and professional of a PT, Advantech entrusts 3rd party CB testing laboratories (CBTLs) to perform the penetration testing.

7 Q&A

7.1 Product Security Management

Have you established a formal cybersecurity management framework covering all products and services throughout their lifecycle?

According to requirements defined in IEC 62443-4-1 SM-1 Development process, a general product development/maintenance/support process is documented and enforced that is consistent and integrated with commonly accepted product development processes.

Refer to 4.1, Advantech got certified of IEC 62443-4-1 with Maturity Level 2 in September 2020.

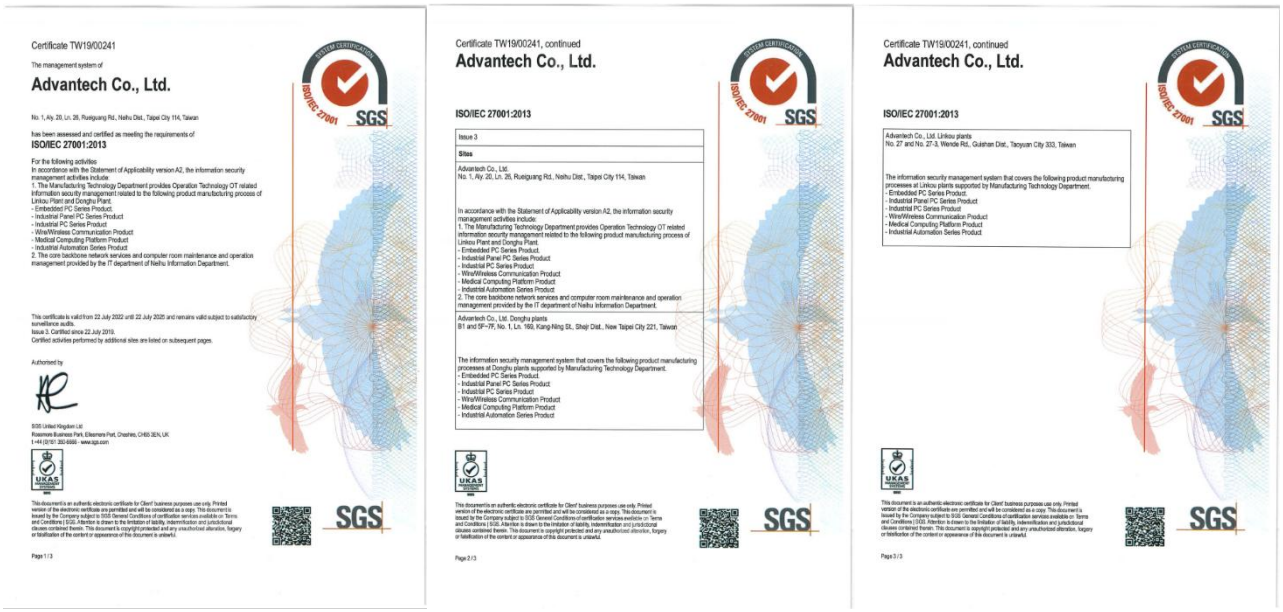
Do you have assigned roles and designated contact persons/channels for cybersecurity and privacy-related issues?

Advantech implements an incident escalation path and breach notification procedure in the official WEB site. It discloses the security advisory also provide the contact window to report a potential vulnerability by mail to ACIRT@advantech.com.

Do you follow cybersecurity standards such as ISO 27001, IEC 62443-4-1, or SOC 2?
Do you have any certifications confirming compliance with industry-specific security regulations and standards?

Refer to 4.1, Advantech got certified of IEC 62443-4-1 with Maturity Level 2 in September 2020.

There's also a certificate for ISO 27001.



Do you provide regular cybersecurity awareness training to employees, including role-specific security training?
Refer to 2.3, Advantech provides ongoing cybersecurity training for all employees, emphasizing the importance of cybersecurity standard compliance.

7.2 Secure Product Development

Do you have a standardized, documented process for cybersecurity tasks and procedures in product development, maintenance, and lifecycle management (Secure Development and Lifecycle Process - SDLC)?
According to requirements defined in IEC 62443-4-1 SM-1 Development process, a general product development/maintenance/support process is documented and enforced that is consistent and integrated with commonly accepted product development processes.

Refer to 4.2, Advantech established the Secure Software Development Life Cycle (SSDLC) with V-model.

Have you defined and documented security requirements (functional and non-functional) for all products? Do you ensure traceability of security requirements across the development process?
According to requirements defined in IEC 62443-4-1 SR-3 Product security requirements, a process is employed for ensuring that security requirements are documented for the product/feature under development including requirements for security capabilities related to installation, operation, maintenance and decommissioning.

Do you have a defined process for secure change and configuration management, including security reviews before deployment?
According to requirements defined in IEC 62443-4-1 SM-1 Development process, a general product development/maintenance/support process is documented and enforced that is consistent and integrated with commonly accepted product development processes which include configuration management with change controls.

Do you follow a structured, security-focused design and implementation process that includes:

- **Threat modeling and security design reviews**
- **Security-by-design principles**
- **Secure coding guidelines**
- **Peer reviews and audits to ensure security of the best practices.**
- According to requirements defined in IEC 62443-4-1 SR-2 Threat model, a process is employed to ensure that all products have a threat model specific to the current development scope of the product.
- According to requirements defined in IEC 62443-4-1 SD-1 Secure design principles, a process is employed for developing and documenting a secure design that identifies and characterizes each interface of the product, including physical and logical interfaces.
- According to requirements defined in IEC 62443-4-1 SI-2 Secure coding standards, the implementation processes incorporate security coding standards that are periodically reviewed and updated.
- According to requirements defined in IEC 62443-4-1 SD-4 Secure design best practices, a process is employed to ensure that secure design best practices are documented and applied to the design process.

Do your development and product lifecycle processes include cybersecurity aspects at all stages and adopt industry best practices for firmware, application, solution, and API design?
Advantech follows IEC 62443-4-1 to establish a Secure Software Development Life Cycle (SSDLC) and adopt industry best practices for firmware, application, solution, and API design to meet requirements defined in IEC 62443-4-2.

7.3 Security Testing

Do you conduct structured security testing as part of your SDLC, including automated and manual security validation (e.g., SAST, DAST, Fuzzing)?
Do you follow the industry's best practices for security testing across all stages of development?
Do you conduct penetration testing on your products, at least upon initial release and major updates?
According to requirements defined in IEC 62443-4-1 Practice 5 Security verification and validation testing, Advantech conducts structured security verification and validation as part of SSDLC, which includes:

- Security Functional Testing: Be verified and validated by Advantech SQA.
- Threat Mitigation Testing: Be verified and validated by Advantech SQA.
- Vulnerability Analysis (VA): Be verified and validated by third-party lab.
- Penetration Testing (PT): Be verified and validated by third-party lab.

7.4 Third-Party Cybersecurity Risk Management

Do you have a structured process for assessing and managing cybersecurity risks in your supply chain? Does it include:

- **Supplier security assessments**
- **Risk Mitigation plans.**
- **Chain of custody verification for third-party components**

According to the requirements defined in IEC 62443-4-1 SM-9 Security requirements for externally provided components, Advantech will sign NDA including relevant security requirements into contract or additional agreement by the responsibilities with the outsourcing vendor.

Advantech evaluates possible potential security risks prior to outsourcing software development to vendors, such as data or user access code, system sabotage or data loss, and other risks. Vendor shall present certificates that guarantee no malicious program codes in the programs delivered.

Do you have an automated process for reviewing and monitoring third-party software dependencies, including SBOMs and vulnerability scans?

Refer to 4.3, Advantech established a SBOM management mechanism to create/refine/review/remediate/monitor and update third-party software components with security patches.

Do you maintain and provide SBOM for your product in a standard format (CycloneDX or SPDX)?

Refer to 4.3, Advantech provides an SBOM for products in a SPDX format.

7.5 Vulnerability Management

Do you have a formal vulnerability management program that identifies, assesses, and mitigates security vulnerabilities in your products? Does it cover both development and aftermarket phase?

Refer to 4.4, Advantech established a vulnerability management mechanism to gather/review/assess/address and disclose vulnerability/CVE based on SBOM or open-source list of the product.

Do you have a responsible disclosure program or bug bounty initiative for external vulnerability reporting?

Refer to 4.4, Advantech publishes the security advisories of product to disclose which manner or countermeasure is made for reducing the risk of vulnerabilities.

Do you have a formal process for notifying customers about security vulnerabilities, patches, and updates?

Refer to 4.4, Advantech timely notifies the customers and come out an update software/firmware.

7.6 Secure Production and Logistics

Do you have a security framework in place to protect product integrity during production, logistics, and distribution?

According to the requirements defined in IEC 62443-4-2 CR 3.10 Support for updates, authenticity and integrity of software update/upgrade is checked by verifying the digital signature provided by product supplier prior to installation.

Do you implement security measures to protect against counterfeit components and unauthorized modifications during manufacturing and distribution?

According to the requirements defined in IEC 62443-4-2 CR 3.11 Physical tamper resistance and detection, Advantech implements the anti-theft screws for tamper resistance and warranty seal for tamper detection.

7.7 Cybersecurity Incident Management

Do you have a formalized security incident management framework?

Do you have clearly defined incident response and breach notification procedures, including response times?

Refer to 2.1, Advantech has established procedures for reporting and handling cybersecurity incidents.

Refer to 3.3, Advantech develops and maintains an incident response plan to manage and mitigate the impact of security incidents. Notify the customer promptly, in accordance with any applicable law or regulation and in any event within 72 hours after discovery of any security incidents or threats.

7.8 Physical Security

Do you have a comprehensive physical security program in place?

Do you implement measures to protect IT infrastructure against unauthorized physical access and environmental threats?

Refer to 3.2, Advantech defined the policy for Physical and Environmental Security.