

How Robust Are Your Cybersecurity Solutions?

From Compliance to Real-World Threats

- Trends & Regulations
- IEC 62443 Standards
- Security Management
- Product Selection Guide

Vertrieb durch



AMC – Analytik & Messtechnik GmbH Chemnitz

Heinrich-Lorenz-Str. 55 Tel.: +49/371/38388-0
09120 Chemnitz Fax: +49/371/38388-99
E-Mail: info@amc-systeme.de Web: www.amc-systeme.de

Why Advantech

Vertrieb durch



AMC – Analytik & Messtechnik GmbH Chemnitz

Heinrich-Lorenz-Str. 55

Tel.: +49/371/38388-0

09120 Chemnitz

Fax: +49/371/38388-99

E-Mail: info@amc-systeme.de

Web: www.amc-systeme.de

At Advantech, we see cybersecurity as a cornerstone of digital transformation. With decades of experience in industrial computing and a commitment to continuous innovation, we lead with a secure-by-design mindset. Our cybersecurity practices align with global standards like IEC 62443 and ISO/IEC 27001, helping customers reduce risk, accelerate compliance, and stay ahead of evolving threats. When security matters, trust Advantech to deliver more than just technology—we deliver peace of mind.



The New Age of Cybersecurity: Are You Ready?

As digital transformation accelerates, cybersecurity threats continue to evolve, driving the need for stringent regulations and proactive security measures. The European Union has introduced critical cybersecurity directives, including NIS2, the Cyber Resilience Act (CRA), and Radio Equipment Directive Delegated Act (RED DA). These regulations highlight the global shift toward stricter cybersecurity governance, urging organizations to adopt robust security frameworks and comply with industry standards.

Regulation	Who is affected?	Which products/sectors matter?	Penalties
NIS2	Companies who operate essential or important IT/OT systems	Sectors that are • Essential for infrastructure (e.g. energy, transport) • Important industries (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

Cybersecurity Standards



NIS2 Directive

The NIS2 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's approach to incident notifications, security requirements, supervisory measures, and information sharing.

NIS2 is about laws and policies that mandate critical infrastructure must have cybersecurity measures appropriate to the threats and must report cyber incidents to the regulatory authority.

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 are mainly hardware and software whose "intended and foreseeable use includes direct or indirect data connection to a device or network".

For the CRA, the 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.



Fortifying Cybersecurity from Within



Cybersecurity Committee (CSC)

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



ISO/IEC 27001

Certified to ISO/IEC 27001, we implement a rigorous, risk-based information security management system that strengthens corporate governance, regulatory compliance, and operational resilience. With a structured security framework and continuous optimization, we ensure a robust foundation for secure and efficient business operations.

Securing the Product Development Lifecycle



Security is integrated into every phase of our product development to identify and address potential vulnerabilities. With IEC 62443-4-1 certification, our Secure Software Development Lifecycle (SSDLC) meets top industrial cybersecurity standards. From development to deployment, our products offer strong protection against cyber threats.

IEC 62443-4-1

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

Secure Software Development Lifecycle (SSDLC)

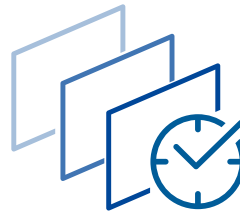
Advantech's SSDLC, based on the IEC 62443-4-1 V-model, integrates security and automation into every phase. With requirement-based testing and thorough validation, it ensures early risk mitigation, faster compliance, and secure, reliable solutions for industrial applications.

IEC 62443-4-2

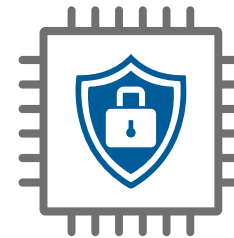
Advantech offers a comprehensive solution to enhance software protection and significantly improve the efficiency of testing and certification. Advantech joins forces with Bureau Veritas, a global leader in testing, inspection, and certification, to help customers overcome security challenges in AIoT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



Simplify security assessments and regulatory compliance



Reduce deployment time by integrating pre-certified, security-hardened solutions



Enhance overall system resilience against cyber threats

Proactive Security Measures to Mitigate Emerging Risks

Security Advisory

Advantech maintains a comprehensive vulnerability management process. The ACIRT (Advantech Cybersecurity Incident Response Team) rigorously assesses potential threats to products and provides 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. [Visit our website](#) to stay tuned and secure.

Software Bill of Materials (SBOM)

In line with IEC 62443-4-1, Advantech has implemented an SBOM management mechanism to track and update third-party components with security patches. SBOM provides full visibility into the software supply chain, helping businesses identify vulnerabilities, ensure compliance, and strengthen cybersecurity. By proactively managing dependencies, organizations can mitigate risks and maintain a resilient, secure development lifecycle.



IEC 62443-4-2 Product Offerings

Modular HMI



Industrial Ethernet Switches



TPC-B300

With Intel Atom® X6425E processor

- Compatible with modular displays (12"-24") featuring slim-bezel, P-CAP touch and high-brightness with 50+ configurations
- DDR4 SODIMM slot (up to 32GB), M.2 Key-M 2280 for SATA SSD, and 2.5" SATA SSD expansion
- 2 x 2.5Gb LAN ports and M.2 Key-E 2230 for WiFi + BT module
- Supports Full-size mini PCIe for iDoor expansion

TPC-B520

With 13th Intel® Core™ processors

- Compatible with modular displays (12"-24") featuring slim-bezel, P-CAP touch and high-brightness with 50+ configurations
- Single DDR5 memory slot supporting up to 32GB with expansion via three M.2 slots (NVMe, WiFi, 5G)
- LAN, POE, isolated serial port and isolated digital I/O via iDoor technology
- USB Type-C supporting USB 3.2, DisplayPort 1.4a and 15W power delivery

EKI-7400 Series

24G + 4G Combo Managed Switches

- 24 x IEEE 802.3 af/at PoE Gigabit ports + 4 x Gigabit Copper/SFP combo ports, provide up to 30Watts per port
- Support VLAN-based network segmentation and enforce security with ACLs and DHCP snooping to prevent malicious access
- Support authentication and identity verification through 802.1X, RADIUS, and MAB
- Redundancy: X-Ring Pro (ultra high-speed recovery time < 20 ms), RSTP/STP (802.1w/1D)

EKI-7700 Series

L2 6/8/10/12/16/20 Port Managed Switches

- Offering a full portfolio with 6, 8, 10, 12, 16, and 20 ports, with optional PoE
- Support VLAN-based network segmentation and enforce security with ACLs and DHCP snooping to prevent malicious access
- Support authentication and identity verification through 802.1X, RADIUS, and MAB
- Redundancy: X-Ring Pro (ultra high-speed recovery time < 20 ms), RSTP/STP (802.1w/1D)

*The product offerings are constantly updated as our portfolio of IEC 62443-4-2 certified products expands.

Vertrieb durch



AMC – Analytik & Messtechnik GmbH Chemnitz

Heinrich-Lorenz-Str. 55 Tel.: +49/371/38388-0
09120 Chemnitz Fax: +49/371/38388-99
E-Mail: info@amc-systeme.de Web: www.amc-systeme.de

ADVANTECH

Enabling an Intelligent Planet



Please verify specifications before ordering. This guide is intended for reference purposes only.
All product specifications are subject to change without notice.
No part of this publication may be reproduced in any form or by any means, electronic, photocopying,
recording or otherwise, without the prior written permission of the publisher.
without prior written permission of the publisher.
All brand and product names are trademarks or registered trademarks of their respective companies.
© Advantech Co., Ltd. 2025