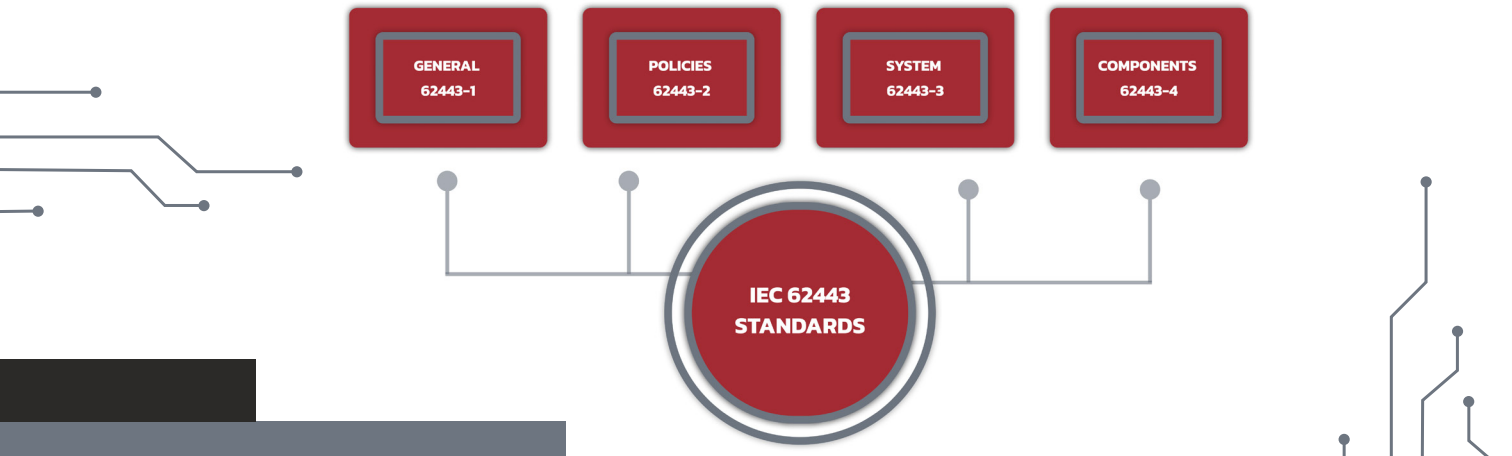
Industrial Control Systems

– ISA/IEC 62443-4-1

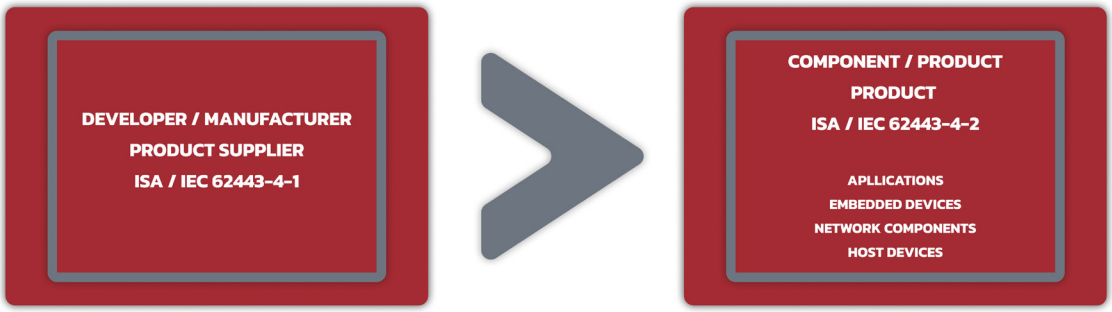
Protecting Industrial Control Systems against cyberattacks became more important than ever before. ISA/IEC 62443 series of standards were created to provide an easy-to-use, achievable model to handle risks and mitigate cybersecurity threats.

EC 62443 is the standard for the protection of Industrial Control Systems and the most effective Cybersecurity solution for Industry 4.0. With increased connectivity of production assets (IIoT), new hazards emerge that need to be included into the traditional risk management processes. An industrial automation control system component manufacturer (supplier) shall include the consideration of security requirements under IEC 62443 4-1 in its product development processes. The IEC 62443 standard Part 4-1 defines a secure development lifecycle for the purpose of developing and maintaining secure products used in industrial automation and control systems (IACS). The IEC 62443-4-1 certificate confirms that the developer has implemented a secure by design methodology from the first day of product development processes, which includes complete security lifecycle and patch management.



TAM CERT Magyarország Kft
www.tamcert.hu

Order to make sure that the security requirements relevant to customers are met, these industrial components shall be certified in accordance with IEC 62443-4-2. If component suppliers follow the set of guidelines that are defined in the IEC 62443-4-2 subsection,they will equip their customers with the best chance of protecting their networks against cyberattacks. Although the component suppliers must add certain features and capabilities to their devices in order for the devices to be suitable for deployment on Industrial IoT networks, conforming to the requirements outlined within IEC 62443-4-2 guarantees secure and resilient components, which are to be procured by 62443 certified and secured IACS organizations.



Security level	Misuse	Means	Resources	Knowledge	Motivation
1	accidental	-	-	-	-
2	intentional	simple	few	general	low
3	intentional	sophisticated	moderate	ACS-specific	moderate
4	intentional	sophisticated	extensive	ACS-specific	moderate

Certification:

The IEC 62443 standard describes 4 levels of security functionality for component security (62443-4-2)

SL1: Protection against causal or coincidental violation
SL2: Protection against intentional violation using sophisticated means with moderatere sources, IACS specific skills and moderate motivation
SL3: Rotection against intentional violation using simple means with low resources, generic skills and low motivation
SL4: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

The Importance of Auditing:

Auditing plays a critical role in maintaining the resilience and security of industrial control systems (ICS). By conducting regular assessments, organizations can gain valuable insights into the strengths and weaknesses of their cybersecurity practices, policies, and procedures. The benefits of auditing in ICS include:

Identifying Vulnerabilities: Audits conducted in accordance with the IEC 62443-4-1 standard help uncover potential vulnerabilities within an organization's control system. By proactively identifying these weak points, companies can take appropriate measures to mitigate risks before malicious actors can exploit them.

Ensuring Compliance: In many industries, such as energy, manufacturing, and critical infrastructure, strict regulatory requirements apply to cybersecurity. Compliance with the IEC 62443-4-1 standard provides organizations with a structured approach to meet these requirements and maintain the necessary certifications.

Enhancing Resilience: Audits contribute to the development of a robust cybersecurity strategy. Organizations can use audit findings to improve their incident response capabilities, business continuity plans, and overall resilience against cyber threats.

Risk Management: Effective risk management requires understanding the threats to ICS. Audits in line with the IEC 62443-4-1 standard help organizations assess the potential impact of various cyber threats and prioritize their security efforts accordingly.

Gaining Stakeholder Trust: Customers, partners, and regulatory bodies often require evidence of effective cybersecurity practices. Compliance with the IEC 62443-4-1 standard demonstrates an organization's commitment to protecting ICS, thereby building trust among stakeholders.

Conducting an Audit According to IEC 62443-4-1:

Defining the Scope: Clearly defining the scope of the audit, including the systems, assets, and processes to be assessed, is crucial for focusing the evaluation and ensuring its relevance to the organization's objectives.

Risk Assessment:
Evaluating the risks associated with each area under review allows the organization to prioritize its efforts and allocate resources effectively.

Evaluation of Security Controls: Auditors examine existing security controls and measures, comparing them against the requirements of the IEC 62443-4-1 standard.

Documentation and Reporting: Detailed documentation of the audit findings and recommendations is essential for organizations to understand their current state of cybersecurity readiness and to develop improvement plans.

Continuous Improvement: Regular audits, ideally conducted at predetermined intervals, enable organizations to track their progress and continuously enhance their cybersecurity posture.

Conclusion:

The IEC 62443-4-1 standard provides a valuable framework for conducting audits of industrial control systems (ICS), offering a structured approach for organizations to evaluate cybersecurity and manage risks. By adhering to this standard, businesses can identify vulnerabilities, maintain compliance, enhance resilience, and build trust with stakeholders. Regular audits conducted in accordance with IEC 62443-4-1 are a proactive step towards protecting critical infrastructure and advancing in the ever-evolving landscape of cybersecurity threats in the industrial sector.

Contact a Trusted Certification Body Accreditation always guarantees preparedness. TAM CERT is an accredited cybersecurity certification body. You can access the designation of accreditation here:

https://nah.gov.hu/admin/staticmedia/Reszletezo_okiratok/RO4-NAH-6-0070-2023-B1-IG-11756640_a.pdf

Contact Us!

Tibor KISS

Head of Cybersecurity Certification

+36 30 5150840

kiss.tibor@tamcert.hu

www.tamcert.hu