TÜVNORD

Inspired by Knowledge

Cybersecurity Management for Industrial Automation and Control Systems (IACS)

Overview: OT security in industrial and regulatory environments

Industrial automation and control systems (IACS) are a central component of modern production, process, and infrastructure landscapes Ongoing digitalization, the use of IoT technologies, remote maintenance concepts, and the increasing convergence of IT and OT are increasing efficiency and transparency – but at the same time significantly increasing the attack surface and cyber risks.

In the industrial environment, the focus is particularly on the security objectives of availability, integrity, and confidentiality of control and process data. Security incidents can have a direct impact on production capacity, product quality, environmental and personal safety, as well as on the economic stability and reputation of a company. At the same time, regulatory requirements and customer and partner demands are increasing the need for a structured, verifiable level of OT security.

The IEC 62443-2-1:2024 (Edition 2.0) standard is the central international standard for operators (asset owners) of industrial automation and control systems. It defines requirements for policies, processes, and organizational measures for a systematic security program (SP) to ensure cybersecurity in the operation of IACS. In the current edition, the term „cybersecurity management system“ (CSMS) has been deliberately replaced by the term „security program“ in order to achieve better alignment with existing information security management systems (ISMS) and to consistently integrate overlaps.

The standard explicitly takes into account the long life cycles of industrial plants and addresses the secure handling of legacy systems through risk-based and compensatory measures. Technical, organizational, personnel, and physical aspects of OT security are considered in an integrated manner and controlled throughout the entire plant and operating life cycle.

With certification according to IEC 62443-2-1, TÜV NORD CERT confirms that the security program has been effectively implemented and that OT cybersecurity has been systematically, risk-oriented, formally and transparently embedded in corporate management.

Key features of IEC 62443-2-1 certification

- Internationally recognized standard for the development and operation of a security program for industrial automation and control systems
- Risk-based, lifecycle-oriented approach to managing IACS cyber risks
- Clear governance structures with defined roles and responsibilities (e.g., asset owner, OT operations, maintenance, service providers)
- Integration of organizational, technical, and process-related security measures
- Continuous improvement process (e.g., PDCA approach) for sustainably increasing cyber resilience
- Good compatibility with existing management systems, in particular ISMS according to ISO/IEC 27001 (e.g., integrated audits, joint governance structures, and synergies in documentation and risk management)

Target groups for certification

Certification according to IEC 62443-2-1 is aimed at organizations with industrial control and automation environments in various industries, sizes, and maturity levels.

Typical target groups are organizations that:

- operate industrial, process, or energy facilities (e.g., manufacturing, chemical, oil & gas, energy supply, water/wastewater, transportation, building technology)
- operate critical infrastructures or high-availability production environments where OT disruptions have a significant impact on safety, supply, or delivery capability
- already operate an ISMS in accordance with ISO/IEC 27001 and want to secure their OT systems in a standard-compliant and verifiable manner
- have to meet requirements for structured OT security management from customers, OEMs, or operators (e.g., as part of supply, operating, or service contracts)
- want to strengthen their cyber resilience, plant availability, and business continuity throughout the entire IACS lifecycle

The standard is suitable for organizations with established management systems (e.g., ISO 9001, ISO/IEC 27001) as well as for companies that want to introduce OT security holistically and systematically for the first time.

Your route to IEC 62443-2-1 certification in 5 steps

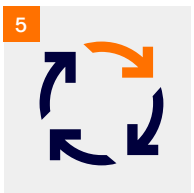
The certification process according to IEC 62443-2-1 follows the proven structure of management system audits and is adapted to the size, complexity, and risk profile of the organization.

Inquiry & offer

Stage 1 Audit – Readiness assessment

Stage 2 Audit – Certification Audit

Certification decision & certificate



Monitoring & recertification

Our know-how for your success

TÜV NORD CERT is an internationally recognized and reliable partner for testing and certification services. Our experts and auditors have in-depth knowledge and generally have a permanent position at TÜV NORD. This ensures independence and neutrality as well as continuity in serving our customers. The benefit to you is clear: our auditors accompany and support the development of your company and provide you with objective feedback.

Contact

TÜV NORD CERT
Building 5, Lane 288
Kangning Road, Jing An
District, Shanghai,
China. 200443

T +86 21-33196200

www.tuv-nord.com/cn

gc-mkt@tuev-nord.de

24-0613-03/26