Add value.
Inspire trust.

IEC 62443 Certification

Enhance the cyber resilience of industrial components and systems

Your challenges

Across a variety of businesses, from manufacturing and processing plants, to energy suppliers and rail, cyber-physical systems are implemented to improve efficiencies, which deliver unmatched flexibility and innovative business models. But, this new connectivity also translates into a shift in the risk landscape, as cyberattacks are increasing. Against this backdrop, suppliers and system integrators must optimise the cyber resilience of their components and systems by improving development, integration and support processes.

Why is industrial security important for your business?

A security breach involving a connected industrial application can put an entire facility at risk – and the consequences for operations, people and equipment could be devastating. As vulnerabilities may appear throughout the component or system lifecycle, it is necessary to plan ahead and implement security from the onset. From specification, to design, production and support, component suppliers must consider how the cyber resilience of a connected device can be optimised for its entire lifespan. Further down the line, the system integrator must take possible threats to the automated solution into account. Consequently, suppliers and integrators are required to mitigate risk, even when the prospective configuration and the potential threats are still largely unknown. Furthermore, transparency is required for a potential buyer to place trust in the security capabilities of product suppliers and integrators.

What is IEC 62443?

Aiming to mitigate risk for industrial communication networks, the international standard IEC 62443 provides a holistic approach to cybersecurity. Originally developed for the Industrial Automation and Control Systems supply chain, it has become the leading industrial cybersecurity standard for all types of plants, facilities and systems across industries. The standard applies to component suppliers, system integrators and asset owners.

Through a set of defined process requirements, the standard ensures that all applicable security aspects are addressed in a structured manner. This includes a systematic approach to cybersecurity throughout the stages of specification, integration, operation, maintenance and decommissioning. Adapted to the relevant project scope, IEC 62443 lays the foundations for cybersecurity throughout the product and system lifetime. Furthermore, a third-party certification demonstrates to asset owners and operators that the purchased component or system is based on a methodised and coherent approach to cybersecurity, in line with industry best practices.

How can we help you?

TÜV SÜD is one of the first companies to provide certifications according to IEC 62443. Suppliers and system integrators worldwide partner with us to confirm their compliance to applicable requirements, as laid out in the standard. The table below summarises the IEC 62443 service portfolio of TÜV SÜD:

	Product supplier		System integrator
Process	IEC 62443-4-1		IEC 62443-2-4
Product	Component	Control system	Blueprint
	IEC 62443-4-1 IEC 62443-4-2	IEC 62443-4-1 IEC 62443-4-2	IEC 62443-2-4 IEC 62443-3-3

For product suppliers, TÜV SÜD provides certification services based on IEC 62443-4-1 -"Secure Product Development Lifecycle". The standard applies to the supplier's security processes which are connected to the development and maintenance of the relevant component and control system.

Corresponding certifications are available to system integrators based on IEC 62443-2-4 -"Security Program for Service Providers". In this case, the compliance of generic intergration processes, as well as compliance of security processes for a reference architecture or blueprint, can be verified by our experts.

Besides the process aspects during product development and system integration, IEC 62443 also specifies technical security requirements for components and systems, which are described in IEC 62443-4-2 and IEC 62443-3-3.

Your business benefits

- **Minimise risk** – enhance cyber resilience of your products and systems through a structured approach to industrial security.
- **Increase competitiveness** – demonstrate your security capabilities by implementing IEC 62443 requirements and industry best practices.
- **Improve customer trust** – apply the globally renowned TÜV SÜD certification mark to confirm your commitment to cybersecurity.

Why choose TÜV SÜD?

Our extensive experience with industrial processes, combined with profound expertise in industrial cybersecurity, makes us uniquely positioned to assess your security processes and solutions. Our methodology for risk analysis, applying both security and safety aspects, is proven in the field. TÜV SÜD experts actively participate in international standardisation committees, gaining valuable insights on the latest regulatory developments. Due to our experts' relentless commitment to instil safe operations across industries, the TÜV SÜD certification mark has become a globally renowned symbol for safety, security and trust.

Add value. Inspire trust.

TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions. It specialises in testing, certification, auditing and advisory services. Through more than 24,000 employees across over 1,000 locations, the company adds value to customers and partners by enabling market access and managing risks. By anticipating technological developments and facilitating change, TÜV SÜD inspires trust in a physical and digital world to create a safer and more sustainable future.

Related services

TÜV SÜD offers trainings, testing, auditing and certification in the areas of:

- Industrial IT Security
- ISO/IEC 27001 information security management
- Functional safety for machinery
- Machinery safety
- Robotic safety
- Wireless communication

TÜV SÜD AG Westendstr. 199, 80686 Munich, Germany
+49 89 5791 0 industrialproducts@tuvsud.com www.tuvsud.com/industrialproducts