IEC 62443 TESTING AND COMPLIANCE

Secura

Who is this for?

- ICS/SCADA products and systems owners, developers and manufacturers
- Medical devices developers and manufacturers

What are the deliverables?

Compliance report and gap analysis

What is the result?

Demonstrated compliance against internationally recognized standard

IN CONTROL WITH SECURA

Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security assessment services varying in depth and scope.

What is IEC 62443?

IEC 62443 is an internationally recognized family of standards providing a complete framework for assessing various actors involved in the field of Industrial Automation and Control (IACS).

Originally designed to be used for Industrial Control Systems (ICS), IEC 62443 is now considered a relevant standard across many industry verticals, due to the holistic way in which its requirements are expressed.

Scope of Evaluation

IEC 62443 is a versatile family of standards, which could be fit to multiple types of stakeholders, involved within multiple industrial domains.

- **ICS manufacturers and owners** involved in process industries such as chemical, oil/gas or transportation can make use of IEC 62443 in order to validate the security of individual ICS systems, or the way in which they are deployed inside the company's network.
- **Medical device manufacturers** can use IEC 62443 for assessing the security features embedded into their devices. In the medical domain, this standard is particularly relevant, since it is recognized by various regulatory institutions (among which the American FDA) for demonstrating compliance with local regulations on medical devices.

For **manufacturers**, compliance to IEC 62443 is a powerful tool for demonstrating the security of their systems and components and enhancing their market advantage. For **asset owners and system integrators**, compliance to the procedures in the standards helps in improving the brand image and minimizing the risk of security breaches. Secura can offer you services for the whole range of standards, such that you can demonstrate your compliance.

Product Specific Compliance

The security of your components and systems is essential for a good brand image and for minimizing possible risks. The following standards can be used in the case of **manufacturers** for validating compliance:

- **IEC 62443-3-3**, assessing the security capabilities of systems. Examples could be SCADA systems, consisting of multiple sensors, control units, HMIs and software applications.
- **IEC 62443-4-2**, assessing the security capabilities of the individual system components. Examples could be local PLCs (programmable logic controllers) or the control unit of a building's smart lights.

Based on the intended scope of evaluation (product specific), Secura will tailor together with the customer the applicable security requirements from the IEC 62443 standard. The assessment will then be performed in line with these selected requirements. IEC 62443-3-3 and IEC 62443-4-2 will be used as a source of testing requirements, providing a complete framework for evaluating the security. The assessment will be finalized with a Compliance Report which is shared with the customer. The report highlights the compliance state of the assessed product against the requirements in scope, as well as identifies and explains the security gaps.

During the security assessment, the following items are examples of tests performed on the product:

- User authentication and authorization controls
- Secure use of component's interfaces
- Secure key management
- Logging of events
- Remote and concurrent sessions management
- Software integrity
- Network and application segmentation
- Timely response to incidents and events
- Resource availability

Process Specific Compliance

Even if the off-the-shelf system is considered secure, the way in which it **is manufactured, installed, used and maintained** is crucial for the security of the whole network. The following standards can be used to assess your systems and procedures:

- **IEC 62443-2-1**, assessing the procedures for establishing and maintaining a security management system within your organization.
- **IEC 62443-2-4**, assessing the ICS systems integration procedures.
- **IEC 62443-4-1**, assessing the secure development procedures implemented by product manufacturers.

Based on the intended scope of evaluation (process specific), Secura will tailor together with the customer the applicable security requirements from the IEC 62443 standard. The assessment will then be performed in line with these selected requirements. Organizations interested in having their internal processes and procedures evaluated can make use of the IEC 62443-2-1 standard. IEC 62443-2-4 is used to assess the processes used by product integrators and service providers. IEC 62443-4-1 can be used to evaluate the secure development procedures associated with a particular product (component or system).

When assessing process specific compliance, an initial documentation review on the processes and procedures is combined with an on-site audit for validating their practical applicability. The assessment will be finalized with a Compliance Report which is shared with the customer. The report highlights the compliance state of the assessed processes against the requirements in scope, as well as identifies and explains the security gaps.

The following topics are examples of activities/targets in the scope of this kind of assessments, also depending on the type of processes analyzed:

- Security management process
- Preliminary risk assessment procedures (e.g. threat modelling, risk levels, residual risks)
- Determination of product security requirements and controls
- Secure architecture design
- Product security documentation
- Secure coding practices
- Security testing on the products by the manufacturer
- Security incident response planning
- Monitoring and incident response

Secura

Insight Into Your Security with Secura

Secura has worked in information security and privacy for two decades. By leveraging our experience and expertise, we are a strong partner to address your information security matters efficiently and thoroughly. We can offer you the following services, in line with the IEC 62443 family:

- **For system and components manufacturers**, product compliance assessment to relevant IEC 62443 standards
- **For system users and integrators**, procedures compliance assessment to relevant IEC 62443 standards
- **For manufacturers, integrators and service providers**, possible certification in line with relevant IEC 62443 standards. For more details, please refer to the separate IECEE certification fact sheet.

Would you like to know more about security testing and/or certifying your ICS/ SCADA product, system or medical device?

Contact us today to discuss our services in more detail and find out which service fits your product best.

Interested?

Would you like to learn more about our services? Contact us today:

Follow us: in 🐦 f

☎ +31 88 888 31 00

✉ info@secura.com

🌐 secura.com