SIEMENS

On line-Training OT Cyber Security e IEC 62443 - corso completo (IK-SECCOM)

Short Description

Module that includes all IEC 62443 topics for a complete course on the standard and all its relevant parts. Starting from the problems of cyber security in the industrial sector and from the typical vulnerabilities and attack methods normally used in the industrial sector, the IEC 62443 regulatory framework will be described. The main role in this scenario will be played by the end user who essentially must protect his own infrastructure according to a risk based approach focused on the assessment of cyber risks and which is implemented in the cyber security management system, the so-called CSMS. The standard also presents technical requirements for infrastructures, control systems and components that are available to integrators and manufacturers for the design and implementation of security requirements. Furthermore, these requirements provide the basis for equipping components and systems with certain security capabilities based on the security level parameter in order to provide integrators and end users with products suitable for integration for defined security objectives. The standard also places great emphasis on the governance part with requirements linked to management systems as regards the end user, the integrator and product development as regards component and system manufacturers.

Objectives

After attending the course you will be able to:
- Know what the mandatory requirements applicable to Cyber Security in the industrial sector are
- Understand how the IEC 62443 standard, the main global reference on the topic, is structured
- Understand that the management of industrial Cyber Security must be approached methodically
- Describe the process described by the IEC 62443 standard, in reference to a company management system
- Understand the objectives and need for a risk assessment in the industrial Cyber Security field
- Determine the safety level of an industrial automation and control system
- Apply the technical requirements related to the protection of an industrial automation and control system
- Understand how to safely develop products and manage integrators and suppliers.

Target Group

The course has a complete content and provides the right level of depth on all the topics of IEC 62443 for all the actors involved. It is suitable for those who need to implement governance systems in the company both at end user, integrator or manufacturer level and for those who need to define and implement technical requirements for architectures, systems and components.

Content

- Cyber Security, differences between OT/IT.
- Reference legislative and regulatory framework.
- IEC 62443 standards framework and cyber security lifecycle.
- End-user side approach, where it all begins: high-level risk analysis, detailed risk analysis and security level determination.
- Dynamics of an attack, methods and tools
- From the integrator to the supplier of automation systems and systems.
- Component, System and automation solution, differences and management methods.
- Technical requirements for components and systems
- Product development lifecycle intended for manufacturers.
- Certification of systems or components.

Prerequisites

No one in particular. Desirable: basic knowledge of automation systems, security principles and management systems.

Note

- The course includes examples, developed on real components and systems, albeit in a laboratory setting.
- During the course, group and individual exercises will be carried out to facilitate and verify the learning of the topics described.
- No documentation is provided.

Type

Online-Training

Duration

16 hours

Language

it