SIEMENS

OT Cyber Security for the End user applying IEC 62443-2 (IK-SEC2)

Short Description

Following the introduction to cyber security in the industrial environment carried out with module 1, we enter into the details of the applicable processes for a end user, as described in IEC 62443, in particular section 2. The standard has a life cycle that includes 3 main phases: that of assessment in which the company becomes aware of the risk deriving from cyber attacks on industrial plants and then assesses the risk through a risk assessment process, that relating to implementation, where the company will have to equip itself with the necessary figures, roles and responsibilities to implement the implementation processes of the technical and organizational measures necessary for the mitigation and management of risks and finally the maintenance part, where through audits and monitoring it is necessary to ensure the effectiveness of the processes implemented. In this module you will see them then the methods of implementing the processes required by the standard within a typical industrial end user, starting from the needs of managing the risk and therefore the problem and focusing on the implementation methods that must concern both the organization part of the management system for cyber security, possibly integrating what is already present in the form of other management systems (eg example ISO 27001), and the implementation part of the technical measures with reference to IEC 62443-3-3 which defines the basic requirements to be implement according to the security level and therefore the required security level.

Objectives

After attending the course you will be able to:
- Understand how to make the company management aware of the cyber risk on plants and how to present a plan and a budget to the management for the management of cyber security in the industrial sector
- Understanding the importance of a risk assessment process as a key element for defining the necessary measures
- Understand the fundamental processes for the implementation of security measures, including emergency ones
- Understand the role of an integrator or service provider and the responsibilities associated with the activities performed
- Understand how to manage the supply chain and the selection of products to be integrated on the plants in relation to security
- Explain what a vulnerability is and how it can be exploited during an attack
- Understand the cyber attack methodologies and tools used
- Understand the importance of human beings and social engineering techniques to steal relevant information

Target Group

This course is intended for personnel called to manage the security aspects at company level and who work with company management systems, for personnel called for the management of automation systems, integrators, and to the supply chain in general to understand the potential needs of an end user.

Content

- IEC 62443-2 and presentation of the 3 phases of life cylce: assessment, implementation and maintenance
- Activities related to risk assessment, from business rationale to high-level and detailed assessment
- The cyber attack, methods of execution and examples
- Social engineering and the human element, as a weak link in the security chain
- Interpret the results of the risk assessment: from the security level, zoning and security requirements
- Reference architectures and security principles
- The key elements of an organization that works by processes. From the definition of roles and responsibilities to training
- Asset management and related documentation and information
- Technical requirements. Definition of the specifications in reference to the security level through the IEC 62443-3-3
- Implementation of measures and plans for the progressive adaptation of the infrastructure
- Business continuity plans
- Obtaining the security level target and verifications
- Maintenance of the level of security through auditing and operational control, monitoring

The course includes examples, developed on real components and systems, albeit in the laboratory.
During the course, group and individual exercises will be carried out to facilitate and verify the learning of the topics described.

Prerequisites

Basic knowledge of automation systems, management systems, with particular reference to security.

Type

E-Learning

Duration

8 hours

Language

en

Fee

3,995 EUR