SIEMENS

Introduction to OT Security according to IEC62443 (IK-SEC1)

Kort beskrivelse

First module of the OT Cyber ??Security series that addresses the problem of cyber security in the industrial field at an introductory level, both from the point of view of mandatory references or not (where the requirements in force in different parts of the world and the regulatory frameworks available with particular reference to the IEC 62443 standard) and from the point of view of the possible implementation methods for the management of industrial cyber security in the company, following the process described in the standard itself. In relation to the application of the latter, the problems faced by end users will be described, who are obviously the main players in the entire process and who need to assess and manage the risk, implementing adequate protection systems. and adopting an organization suitable for the effective functioning of the processes, all in line with the level of risk identified. Subsequently, we will move on to describe what is required of the other actors involved in the process, from integrators and those who provide assistance and maintenance services on automation systems, up to the manufacturers of systems and components who, through the provision of products with declared security performances, are called to contribute to the security level of industrial automation systems, according to the needs of end users.

Målsætninger

After attending the course you will be able to:
- Know what are the mandatory requirements applicable to cyber security in the industrial sector
- Understand how the IEC 62443 standard, the main world reference on the subject, is structured
- Understand that the management of industrial cyber security must be approached methodically
- Describe the process described by the IEC 62443 standard, with reference to a business management system
- Understanding the objectives and the need for a risk assessment in the field of industrial cyber security
- Determine the safety level of an industrial automation and control system
- Understand what tools are available for risk mitigation
- Apply the technical requirements related to the protection of an industrial automation and control system
- Determine the processes necessary for the management of security issues

Målgruppe

This course is intended for a multidisciplinary audience made up of participants who manages cybersecurity requirements in the company, such as sales offices, product managers, technical offices, quality, human resources, purchases, service and technical support.

Indhold

- Cyber Security, differences between OT / IT.
- Legislative and regulatory framework of reference.
- IEC 62443 standards framework and cyber security lifecycle.
- The roles involved.
- End-user approach, where it all begins: high-level risk analysis, detailed risk analysis and security level determination.
- Dynamics of an attack, methods and tools
- Security seen as an effective combination of adequate technical countermeasures and effective processes
- From the integrator to the supplier of automation systems and systems.
- Component, System and automation solution, differences and management methods.
- The development of safe products
- Certification of systems or components

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.

Deltagerkrav

None.
Basic knowledge of automation systems, security principles and management systems are recommended.

Type

E-learning

Varighed

8 timer

Sprog

en

Gebyr

3.995 DKK