Fundamentals of Industrial Security

Fundamental

Objective

Digitisation, networking of machinery and digital elements in automation require Industrial Security to be considered in order to protect machinery. The aim of this training is to build up basic knowledge of Industrial Cyber Security: Basic terminology, concepts and regulatory requirements enable participants to access the subject through clear, practical examples, and communicate basic specialist knowledge of cyber security in the machinery sector. Specific topics in the area of network technology lead to a deeper technical understanding. Cyber attack scenarios and typical behaviours of hackers in industry are described, while risk reduction options, particularly on machinery, are also presented.

As a result, this Industrial Cyber Security Training provides an optimum basis for acquiring the knowledge needed to improve the security of your own industrial plant and machinery. Theoretical expertise is combined with practical examples and best practice, to increase protection, particularly against cyber threats.



Contents

- Introduction and fundamentals of Industrial Security
  - Distinction between Operational Technology (OT) and Information Technology (IT)
  - Basic terms and concepts
- Network security
  - Explanation of terms and components such as routers, switches and protocols
  - Network architecture
  - Physical security measures
  - Use of secure protocols and encryption technologies
- Legislation and standards
  - Overview of key standards, such as EN IEC 62443
  - Introduction to the new legal requirements and changes
- Threats and protective measures
  - Examples of actual cyber attacks
  - Introduction to attackers' techniques
  - Impact of attacks on industrial systems
  - Generic risk minimisation measures
- Security concepts and strategies
  - Development of security concepts and strategies in industrial automation
  - Principle of "Defence in Depth" as a multi-layered security strategy
  - Explanation of how to implement an Industrial Security concept based on a risk evaluation

Fundamental

Target groups

This training is aimed at all employees of machine manufacturers, integrators and operators who are looking for an introduction to the subject of Industrial Security. The training is particularly suitable for those who are responsible for Machinery Safety in day-to-day operations, such as:

- Design engineers
- Project managers
- Planners
- System integrators
- Safety officers
- Production managers/those responsible for production
- Those responsible for upgrades and maintenance of plant and machinery
- Technical purchasers

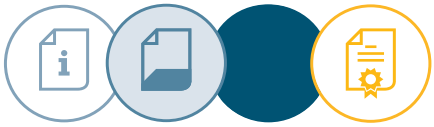
Note

The “Fundamentals of Industrial Security” training course is the ideal preparation for the expert training CESA – Certified Expert for Security in Automation. The training is provided in both classroom and online format with a live instructor. For online training, a laptop equipped with a webcam, and Google Chrome or Microsoft Edge is required to participate.

Benefits to you

- Quick introduction to the subject of Industrial Security, covering the most important principles, terms and specialist knowledge
- Compact knowledge-building, covering the requirements and all relevant aspects of Industrial Security
- Practical reference by analysing actual cyber attacks
- Learn about the latest relevant standards and legal requirements

Your optimum qualification path:



Introduction: Safety Meets Security

Fundamental: Fundamentals of Industrial Security

Expert: CESA – Certified Machinery Safety Expert

Note: *Most Pilz UK courses, including this one, can be hosted at external locations. Travel expenses for the trainer would be included in the cost.*

Course Details:

Duration:	**1 day**
	9:00 – 17:00
Fee:	**£500 +VAT per person**
Number of participants:	Up to 10