COURSE DESCRIPTION

T154 TÜV Rheinland Cyber Security Specialist Cyber Security related to the “Fundamentals of Cyber Security” Four Day Training Course

The goal of this course is to provide an appreciation and awareness of the key organisational and technical requirements for the implementation of robust cyber security lifecycle management in the context of Industrial Automation Control Systems.

Course goal

The goal of this course is to learn the fundamental principles and technical requirements for security & cyber security in the context of the management, technical, specification, design, operation and maintenance of Industrial Automation Controls Systems (IACS).

Course attendance is open to all interested parties and achieving the threshold mark for the examination will result in the candidate receiving a *“TÜV Rheinland SySec Specialist”* attendance certificate.

Learning objectives

Upon completion of this course, the participants will be able to:

- Describe the principles of security and cyber security management and the key features of Industry standards and technical reports
- Understand the fundamentals of communication networks and relevant technology
- Understand the requirements for communication protocols, routing and segmentation
- Outline the key deliverables from the cyber security risk assessment in terms of technical countermeasure specification, design, operations & maintenance regarding cyber security lifecycle phases, and roles and responsibilities

- Understand the requirements for organisational security, business impact, planning and recovery in terms of policy, procedures, guidelines and competency requirements
- Understand the requirements for proper inspection, operation, maintenance and modification of installed cyber security measures as required by the safety & security standards

Participant profile

This training is targeted to engineers, managers, consultants and specialists who require a general introduction & awareness to the relevant industry standards and the key requirements for cyber security lifecycle management and compliance from within the following process industry user groups:

- Asset Owner/End User
- Engineering Contractors/EPCs
- Power & Automation System Integrator's
- Service Providers
- Product Manufacturers

The course is particularly useful for those managers and engineers who may be directly or indirectly, involved in executing projects and/or operating and maintaining such IACS requirements covering the entire security & cyber security lifecycle, with a particular focus on physical and cyber security technical lifecycle management.

Course type

This is an instructor-led course with classroom discussions regarding the implementation of cyber security in the context of relevant industry standards and technical implementation requirements. On completion of the course, delegates can sit the examination and for those that are successful, a "TÜV Rheinland SySec Specialist" attendance certificate will be issued.

Topics covered:

- Background on cyber security standards and industry guidance
- Network fundamentals and associated technology
- TCP/IP fundamentals, routing and segmentation
- Technical security. authentication and encryption
- Organisational security and lifecycle management
- Employee awareness & security goals
- Technical countermeasures & implementation
- Relationship to functional safety
- Formal Examination

How to order

Please contact ABB University as listed below for either attendance at any Open course being planned in your region or if you would like to run a training course specific to your organisation.
For on-site training, a fixed price training proposal will be issued to you for your approval to proceed.

Contact

ABB University
https://new.abb.com/service/abb-university
ABB University Course Code - T154
Phone +44 (0) 1785 285 939
E-Mail: oilandgas@gb.abb.com

Course outline

Day 1

- **Course overview**

- Cyber security standards and industry guidance

- Information Security Management Systems

- Policies
- Guidelines
- Risk assessment
- Defense in Depth
- Process

- Asset management, employee awareness & security goals

Day 2

- Network Fundamentals

- Ethernet
- Fibre optics
- SHDSL
- Network Structures

- TCP/IP Fundamentals

- ISO/OSI Layer Model
- IPv4 address and subnetmask
- Routing and Segmentation
- Protocol architecture TCP/IP

Day 3

- Technical security, authentication and encryption

- Firewall (transparent/routing/port filters)
- Passwords and Factor Authentication
- Digital signatures
- Network Planning

Day 4

- **Organisational Security**

- Change management
- Patch management
- Disaster Recovery & Backup
- Handling of portable media

- Examination