TÜVRheinland®
Precisely Right.

VIRTUAL TRAINING COURSE

TÜV Rheinland cyber security risk assessment (T263)

A four day course to learn the principles of cyber security risk assessment for Industrial Automation Controls Systems (IACS)

10-14 October 2022 - Virtual classroom
24-27 April 2023 - Virtual classroom
20-23 November 2023 - Virtual classroom

TÜV Rheinland cyber security risk assessment (T263)

The aim of this course is to learn the fundamental principles for cyber security in the context of the risk assessment method to be applied in the process industries according to IEC 62443 and to understand the role and the process of Security Risk Assessment (SRA) in gaining an understanding of the security risks on the facility and their potential consequences.

The training will further establish the concept of Security Level Targets (SLT) and the Cyber Security Requirements Specification (CSRS). This will also include the relationship between the SLT and the CSRS to the design and implementation of security countermeasures that are capable and able to achieve the security requirements needed of the determined security level for Industrial Automation Controls Systems (IACS).

Course attendance is open to all interested parties and achieving the threshold mark for the examination (in combination with already having successfully passed the examination for the TÜV Rheinland fundamentals of cyber security training course) will result in the candidate receiving a 'TÜV Rheinland Cyber Security Specialist RA' training certificate.

Duration
4 days

Price
£1,700 +VAT

Learning objectives
Upon completion of this course, the participants should be able to understand:
- The requirements for IACS security in the context of relevant standards and cyber security frameworks
- The most common approaches that are available to achieve security and what activities must be carried out
- How SRA is carried out and the relationship to the IACS zones and conduits

Topics covered:
- Background on cyber security standards and industry guidance i.e. IEC 62443
- Introduction to IACS security and the relevant standards and regulations
- Approach to ensuring cyber security asset inventory
- Introduction to Security Risk Assessment (SRA)
- High-level SRA requirements
- Allocation of IACS to zones and conduits
- Detailed-level SRA requirements
- Determining the level of security risk and the security level
- Risk management
- Monitoring and review

Participant profile

This training is targeted to engineers, managers, consultants and specialists who require a general introduction and awareness to delivering a high-level IACS cyber security risk assessment from within the following process industry user groups:

- Asset owner / end user
- Engineering contractors / EPCs
- Power and 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 with a particular focus on the requirements and arrangements for conducting appropriate cyber security risk assessments.

Course type

This is 3 day 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, and on the 4th day, delegates can sit the examination and for those that are successful, a 'TÜV Rheinland Cyber Security Specialist RA' training certificate will be issued.

Agenda
Day 1
Course overview
Introduction to IACS Security Risk Assessment (SRA)
Requirements for cyber security in the IACS environment
Cyber security requirements from IEC 61511 and the NIS directive
Asset inventory
High-level Security Risk Assessment
Day 2
High-level Security Risk Assessment - Required outputs
Allocation of zones and conduits
Detailed-level Security Risk Assessment
Day 3
Risk matrix and security levels
Gap analysis of security countermeasures
Risk management security countermeasures
Detailed-level Security Risk Assessment
Risk management acceptance and documentation
Day 4
Examination

ABB reserve the right to amend the agenda.

How to book
Please contact ABB 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.

ABB technical training
Email: jackie.kendall@gb.abb.com
Phone: Jackie Kendall on +44 (0)1642 372121

Email: emily.lockley@gb.abb.com
Phone: Emily Lockley on +44 (0)1785 285939

Web: www.abb.com/uk/consulting/training
Web: www.new.abb.com/service/abb-university

ABB Limited
Daresbury Park
Daresbury
Warrington
Cheshire
WA4 4BT
United Kingdom
Phone: +44 (0)1925 741111
E-Mail: contact@gb.abb.com

ABB Limited
Pavilion 9
Byland Way
Belasis Business Park
Billingham
Cleveland
TS23 4EB
United Kingdom
Phone: +44 (0)1642 372000
E-Mail: contact@gb.abb.com

ABB Limited
Hareness Road
Altens Industrial Estate
Aberdeen
AB12 3LE
United Kingdom
Phone: +44 (0)1224 592123
E-Mail: contact@gb.abb.com

ABB Limited
Howard Road
Eaton Socon
St Neots
Cambridgeshire
PE19 8EU
United Kingdom
Phone: +44 (0)1480 475321
E-Mail: contact@gb.abb.com

abb.com