TÜV Rheinland Cyber Security Training Program
Security Risk Assessment

The TÜV Rheinland Cyber Security Training Program is a unique opportunity to provide evidence of competency in Cyber Security from an internationally recognized organisation. The CySec Specialist (TÜV Rheinland) certificate program demonstrates competency with respect to assessing and specifying Industrial Automation Control and Safety System (IACS) Security and provides a skill set enabling staff to fulfill responsibilities and to perform activities to recognised standards of competence, in order to:

- *reduce the risk of a successful cyber attack*
- *satisfy legal and regulatory requirements*
- *meet the organisation's system security and business objectives*

By understanding:

- The principles and concepts in the internationally agreed standard IEC 62443
- The concepts and principles behind international standards that cover the area of cyber security and how and when to apply them including:
  - Security Risk Assessment (SRA) - IEC 61511-1 2nd Edition
  - Cybersecurity Management System (CSMS) and SRA – IEC 62443
  - Network and Information Systems (NIS)
- Defining Tolerable risk criteria for Security
- The concept and principle of reducing risks to As Low As Reasonably Practicable (ALARP)
- Understanding how and when to apply qualitative, semi quantitative and quantitative risk assessment techniques and methods
- How to calibrate, prepare and apply popular security risk determination methodologies, such as Attack Trees.
- The Interface between SRA and the Cybersecurity Requirements Specification

Course Objectives

The objective of the course is to provide participants with a fundamental understanding of the principles of IACS Cybersecurity Risk Assessment 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 concept of Security Level – Targets (SL-T) and the Cyber Security Requirements Specification (CSRS)
- The relationship between SL-T and 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

Successful participants, who have sufficient experience and have passed both the Cybersecurity fundamentals and Security Risk Assessment exams, will be eligible for the prestigious CySec Specialist (TÜV Rheinland) certificate in Security Risk Assessment.

The course is based around a practical case study that will be developed across the three days of the course taking the delegate through the SRA process. The course is a modular structure of classroom tuition followed by a case study practical, which will take the participant through the SRA process as identified in IEC 62443-3.2.

Day four consists of a three-hour examination based on a mixture of multiple choice and open SRA questions.

Day 1 Agenda

Provides an introduction to the background, concepts and principles to be applied to the Security risk assessment, competency, compliance, security management and the relevant international standards. The Security Risk Assessment using a risk matrix will be discussed as well as the introduction to the case study

The topics covered are:

- Introduction to TUV Rheinland Cyber Security (CySec) Program
- Requirements for Cyber Security in the IACS environment, including IEC 61511 and the Network and Information Systems (NIS) directive.
- Security Management and Common Management Systems
- Introduction to Security in the IACS environment
- Introduction to the relevant Security and Safety Standards
- Introduction to the IEC 62443 Security Lifecycle
- Introduction to Risk Assessment specific standards
- Asset Inventory and it's relation to Security Risk Assessment

- Introduction to the Case Study
- Asset Inventory exercise – Session 1
- Types of Risk Assessment – Quantitative, Semi Quantitative & Qualitative
- High-Level Security Risk Assessment
    - How to use previous Process Hazard Analysis (PHA) as an input to High-Level SRA.
    - Determination of the High-Level Threat Scenarios
    - Determination of the High-Level Vulnerabilities
    - Determination of the High-Level Risk
    - Determination of the preliminary Security Level - Target
- High-Level SRA exercise – Session 2

Day 2 Agenda

Further develops on the concepts, principles and techniques carried out in day one and the case study work by taking the output from the High-Level SRA and evaluates the risks based on their likelihood and consequence and prioritises them for examination in the Detailed-Level SRA. The second day also includes an explanation of what outputs would be expected from the High-Level SRA. The principles and activities of the Zoning and Conduit sections of the IEC 62443 will also be explained.

The topics covered are:

- The required outputs from the High-Level SRA
- Requirements of IEC 62443 with relation to the Zone and Conduit exercise.
- Trust Boundaries, Entry Points and further benefits of the Zone and Conduit exercise.
- Allocation of IACS to Zone
    - Network Segmentation
    - System Architecture
- Allocation of Zones Exercise – Session 3

Day 3 Agenda

Develops on the case study work carried out in day one and two taking the outputs from the High-Level SRA and the Zone and Conduit exercise and then examining the prioritised risk zones in detail in the Detailed-Level SRA. Also covered is the relation between the Detailed-Level SRA and Attack Trees and how they may be used in both the

risk assessment and the effective implementation of the countermeasures/security controls.

. The topics covered are:

- IEC 62443 Detailed-Level SRA requirements
- Description of Attack Surfaces in the ICS Environment
- Detailed-Level SRA Process
    - Determination of Threats including Threat Assessment
    - Determination of Vulnerabilities including Vulnerability Assessment
    - Determination of the Detailed Risk and Security Level - Targets through the use of a Security Risk Matrix.
- The Importance of Security Level - Targets and their relation to Foundational Requirements.
- How pruning of Attack Trees can be used to demonstrate a Risk-Based approach to risk reduction
- Detailed-Level SRA exercise – Session 4
- Risk Management (Acceptance)
- IEC 62443 Required Documentation for SRA, including the Cybersecurity Requirement Specification (CRS).
- Risk Management (Monitoring and Review)
- Concluding remarks
- Format of exam and preparation and close.

Day 4 Agenda

A three (3) hour competency examination compromising 30 multiple-choice questions (1 mark per question) and open questions 10 questions (4 marks per question).

The pass score criterion is 75% on each paper

Who Should Attend?

Functional, Process and Technical Safety Engineers, Control and Instrument Engineers and Managers, Process Engineers, Operations personnel and managers, maintenance staff, consultants, advisors and persons involved in management, engineering, operations and safety of process operations as well as persons with PH&RA experience and who are

currently involved process hazard and risk analysis, and will be required to take part in the Security Risk Assessments and Cybersecurity requirements specification.

Participant eligibility requirements

In accordance with the TÜV Rheinland Functional Safety and Cyber Security Training Program:

- A minimum of 3 to 5 years' experience in a related field (e.g. Control & Instrumentation, process engineering, IT/OT, functional safety or cyber security).
- University degree or equivalent engineering experience and responsibilities as certified by employer or engineering institution.

Course Provider

EFSTAS Limited

Prices: From £1950 GBP per participant

Contact: Carol Easton, Tel: +44 (0) 1642 715346 or Email: info@efstas.com