TÜV Rheinland Cyber Security Training Program
Cyber Security Fundamentals

The TÜV Rheinland Cyber Security Training Program is a unique opportunity to provide evidence of competency in Cyber Security from an internationally recognized organisation. Successful delegates, on completion of the fundamentals course and exam, will receive a "certificate of completion" from TÜV Rheinland, which will allow them to progress to either the Cyber Security Risk Assessment or Cyber Security Component training.

Successful completion of the full certificate program, completion of the fundamentals course and exam and either the Security Risk Assessment or Component course and exam, will result in the award of the CySec Specialist (TÜV Rheinland) certificate. This award demonstrates competency with respect to either assessing and specifying Industrial Automation Control and Safety System (IACS) Security or product 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.*

The Fundamentals element of the qualification covers gaining a basic knowledge of:

Industrial Protocols, Networks and Networks Security types, ISO/OSI Reference Model Cryptography, IEC 62443 Framework, NIST Cyber Security Framework (CSF), Establishing an Industrial Automation and Control Systems Security Program, Risk Analysis, Addressing Risk with the CSMS and Monitoring and Improving the CSMS.

Course Objectives

The objective of this course is to provide participants with a basic understanding of cyber security fundamentals so as to be equipped to better understand the principles and practices introduced in the advanced IACS Cybersecurity Risk Assessment training course according to IEC 62443 or the IEC 62443-4 Cybersecurity Component course of the TÜV Rheinland Cyber Security Training Program .

Easton Functional Safety Training and Services Limited.
Incorporated in England with Limited Liability. Registered No. 8874608
Springboard Business Centre, Ellerbeck Way, Stokesley, North Yorkshire, TS9 5JZ Telephone: 01642-715346   Internet: www.efstas.com
Registered Office: School Cottage, Ingleby Greenhow, Great Ayton, Middlesbrough, Cleveland TS9 6LL

The course is of modular classroom tuition structure followed by a 90-minute exam.

Successful delegates, on completion of the fundamentals course and exam, will receive a "certificate of completion", from TÜV Rheinland.

Day 1 Agenda

- Industrial networks vs. Business networks
- Network types
- ISO/OSI Reference Model
- OSI Layer 1: Physical
- Layer 2 Switches
- IPv4 Addressing
- Network Address Translation (NAT)
- DHCP

Day 2 Agenda

- Routers
- Layer 3 Switches
- TCP – Connection Oriented Session
- User Datagram Protocol (UDP)
- Firewalls
- Cryptography
- Remote Access VPNs
- Intrusion Detection Systems

Day 3 Agenda

- Modbus
- Profibus
- IEC62443 Framework
- NIST Cyber Security Framework (CSF)
- Establishing an Industrial Automation and Control Systems Security Program

- Risk Analysis
- Addressing Risk with the CSMS
- Monitoring and Improving the CSMS

Day 4 Examination

A 90-minute exam competency examination compromising 75 multiple-choice questions (1 mark each question)

The pass score criterion is 75%

Who Should Attend?

Functional, Process, Technical Safety and Product Design Engineers, Control and Instrument Engineers and Managers, Process Engineers, Operations personnel and managers, maintenance staff, consultants, advisors and persons involved in product development, management, engineering, operations and safety of process operations who require an understanding of the fundamentals of cyber security and who may wish to progress to take part in the TÜV Rheinland CySec Security Risk Assessment or Product Design and Development courses and exam.

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