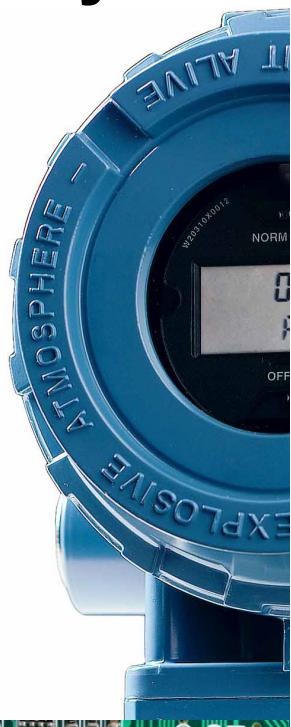
Functional Safety & Cyber Security Training & Workshops



Select the right course for your organisation from our extensive choice of Functional Safety and Cyber Security related training courses and workshops:

Safety Instrumented Systems:

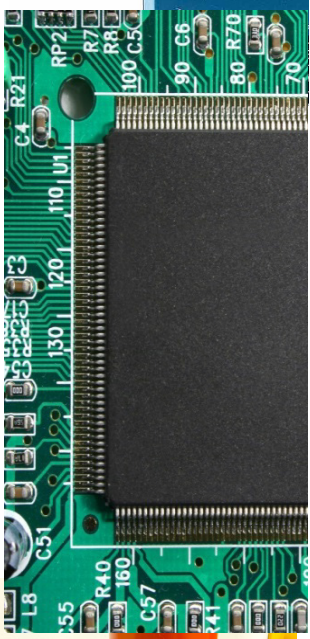
- *FS Engineer (TÜV Rheinland) SIS*
- *FS Technician (TÜV Rheinland) SIS*
- *Introduction to Functional Safety Workshop*
- *SIL Determination Workshop*
- *SIS Design and Development Workshop*
- *Alarm Rationalisation Workshop*
- *Layer of Protection Analysis (LOPA)*

Process Hazard and Risk Analysis:

- *FS Engineer (TÜV Rheinland) PH&RA*

TÜV Rheinland Cyber Security Program – Security Risk Assessment:

- *CySec Specialist (TÜV Rheinland) SRA*



For further information:
E: info@silsupport.com
T: +44 (0) 13398 86618
W: www.silsupport.com

C&C TECHNICAL SUPPORT SERVICES

TÜVRheinland®
Precisely Right.

to obtain your:
FS Engineer or FS Technician (TÜV Rheinland) Certificate
C & C Technical Support Services is an accepted course provider of the TÜV Rheinland Functional Safety Training Program.

Strathayr, Rhu-Na-Haven Road, Aboyne, AB34 5JB, UK
Tel: +44 (0)1339 886618 www.silsupport.com

CONTENTS

Page:

TÜV Rheinland Functional Safety Engineer Safety Instrumented Systems Training (4 days)

General information about this training

This 4 day FS Engineer (TÜV Rheinland) SIS course is run in accordance with the TÜV Rheinland Functional Safety Training Program and comprises three days of classroom tuition and practical guidance, for understanding and mastering the application, principles and requirements of IEC 61508 / IEC 61511. There is a five hour competency assessment on the fourth day. Practical exercises are performed throughout the course based on real life examples.

The assessment on the last day is in two parts with:

70 multiple choice questions (1 mark each question)
10 multiple part questions (3 available marks per question)
Pass score requirement is 75%

Course Objectives

Led by a TÜV Rheinland Functional Safety Expert, this FS Engineer (TÜV Rheinland) certificate course will equip participants with the knowledge for understanding and mastering the application, principles and requirements of IEC 61508 – Functional Safety of electrical/electronic/programmable electronic safety systems and IEC 61511 – Functional Safety: Safety Instrumented Systems for the Process Sector.

Who should attend?

Instrument Engineers, Process Engineers and Process Safety Engineers as well as Senior Operating and Maintenance personnel who are involved in any of the lifecycle phases for safety instrumented systems from hazard and risk assessment, shut down system/fire and gas systems design to testing and maintenance.

Eligibility requirements

In accordance with the TÜV Rheinland Functional Safety Training Program:

- A minimum of 3 years of experience in the field of functional safety and safety instrumented systems;
- University degree or equivalent engineering diploma, or experience and responsibilities as certified by employer or engineering institution.

Certificate

Successful participants, who must also have a minimum of 3 years functional safety experience, will achieve the prestigious FS Engineer (TÜV Rheinland) SIS certificate. All FS Engineers of the TÜV Rheinland Functional Safety Training Program are also listed on the TÜV Rheinland Certipedia Database: www.certipedia.com.

Section 1 Agenda

Will cover process hazard analysis and associated risk management using the most popular and internationally adopted methods and tools. Such hazards can lead to loss of

life, asset damage, loss of production and profitability, damage to the environment and company reputation. Participants will be introduced to the concepts of the main international standards that cover this area of risk assessment and risk reduction.

Content:

- EC 61508 and IEC 61511 background;
- Hazards, Risk and ALARP principles;
- Risk Reduction and mitigation;
- Safety Instrumented System (SIS) and Safety Instrumented Functions (SIF);
- Types of SIF;
- Primary and Secondary Functions;
- Integrity specification of a SIF;
- SIL Determination by risk graphs;
- SIL Determination Exercises;
- Risk Graph Calibration;
- Layer Of Protection Analysis (LOPA);
- SIL determination using LOPA;
- LOPA Exercise;
- Risk reduction >10,000 times using instrumented layers;
- Fault Tree Analysis (FTA);
- SIL Determination by (FTA);
- Case Studies with typical findings and issues.

Section 2 Agenda

During this Section delegates will be taken through the requirements for a Safety Requirements Specification (SRS) and shown how to undertake appropriate cost effective designs for Safety Instrumented Systems (SIS) and Safety Instrumented Functions (SIF) and how optimal test and maintenance strategies for them can be achieved. Participants will be instructed in methods for calculating the probability of failure on demand (PFD), the probability of dangerous failure per hour (PFH), safe failure fraction and hardware fault tolerance. The concepts of failure modes, reliability and the influence of common cause failures will also be covered.

Content:

- SIS Safety Requirements Specification;
- Selection of Components and Subsystems;
- Proven in use (Prior Use);
- Field Devices used in SIS;
- Systematic Failures;
- Random Failures;
- Failure and Reliability;
- Demand Modes;
- Probability of Failure on Demand (PFD);
- PFD Exercises;
- SIF Implementation (Low demand mode);
- Importance of Testing and Maintenance;
- Fractional Dead Times;
- Maximum Time Out of Service;
- Partial Closure Testing of Valves;
- The Impact of Common Cause and Common Mode Failures;
- Safe Failure Fraction and Hardware Fault Tolerance;
- SFF Exercises;

- Calculating PFD for Low Demand Systems with Diagnostics;
- Calculating PFH for High and Continuous Demand Systems with Diagnostics;
- Reliability Data

Section 3 Agenda

Section 3 will look at the application software requirements for safety instrumented systems (SIS) and the relationships between hardware and software architecture. This will include the development of application software specification, module testing requirements and integration with other SIS subsystems. This final day of tuition will also include techniques for undertaking more advanced SIL determination and methods for solving more complex safety instrumented functions.

Content:

- Software requirements;
- Relationships between Hardware and Software Architecture;
- Application Software Requirements Specification;
- Application Software Validation Planning;
- Requirements for Application Software Architecture;
- Requirements for Support Tools, User Manuals and Application Language;
- Requirements for Application Software Development;
- Requirements for Application Module Testing;
- Integration of Application Software with SIS Subsystems;
- Requirements for Application Module Testing;
- Integration of Application Software with SIS Subsystems;
- FPL and LVL Software Modification procedures;
- Application Software Verification;
- Factory acceptance Testing;
- Installation and Commissioning;
- Site Acceptance Testing and SIS Validation;
- Fire and Gas Systems;
- SIS Overrides;
- Further Maintenance Considerations;
- Modifications and Change Control;
- Document Control;
- Course summary.

Final Day Agenda

A five (5) hour two part proficiency assessment comprising:

- Part 1 = 70 multiple choice questions (1 mark each question);
- Part 2 = 10 multiple part questions (3 marks each question).

The pass score criterion is 75%.

TÜV Rheinland Functional Safety Engineer Process Hazard and Risk Analysis Training (5 days)

General information about this training

This 5 day FS Engineer (TÜV Rheinland) PH&RA course is run in accordance with the TÜV Rheinland Functional Safety Training Program and comprises four days of classroom tuition and practical guidance, for understanding and mastering the application of process hazard analysis and associated risk assessment, as required for the early lifecycle phases of IEC 61508 / IEC 61511. There is a five hour competency assessment on the fifth day. Practical exercises will performed throughout the course which will be based on real life examples.

The assessment on the last day is in two parts with:

- 70 multiple choice questions (1 mark each question)
- 2 multiple part questions (30 available marks)
- Pass score requirement is 75%

Course objectives

The topics cover the concepts of identifying hazards, using tools such as What-If, HAZAN and HAZOP. This will be further developed into the assessment of risk and methods of risk reduction using preventative and mitigating layers of protection.

The use of Safety Integrity Levels (SIL) and SIL determination using internationally agreed methods for assessing and quantifying process risk and risk reduction requirements will be introduced. Delegates will be equipped with the knowledge and methods for undertaking various types of qualitative, semi quantified and quantitative risk assessments.

Qualitative methods such as risk graphs and matrices will be introduced and used in practical exercises. The most popular semi quantified method of Layer of Protection Analysis (LOPA) will be fully explored with supporting exercises.

In addition, delegates will be equipped with the knowledge and methods for undertaking various alternative methods of hazard analysis and risk assessment such as such as What-If Hazard Analysis, Failure Mode and Effect Analysis (FMEA, Event Tree Analysis (ETA) and Fault Tree Analysis (FTA).

Delegates will be taken through the requirements for safety management and the framework of a Safety Management System (SMS) for achieving effective process risk management for a green field (new) project lifecycle.

Throughout the workshop, emphasis will be placed on experience and realistic practical exercises and case studies will be used to compliment the instruction.

Who should attend?

Process Engineers, Safety Engineers, Instrument Engineers and Operations personnel who are involved in maintaining the integrity of their processes, and are more involved the early lifecycle phases of functional safety management.

Eligibility requirements

In accordance with the TÜV Rheinland Functional Safety Training Program:

- A minimum of 3 years of experience in the field of process hazard analysis and risk assessment;
- University degree or equivalent engineering experience and responsibilities as certified by employer or engineering institution.

Certificate

Successful participants, who must also have a minimum of 3 years of experience in the field of process hazard analysis and risk assessment, will achieve the prestigious FS Engineer (TÜV Rheinland) PH&RA certificate. All FS Engineers of the TÜV Rheinland Functional Safety Training Program are also listed on the TÜV Rheinland Certipedia Database: www.certipedia.com.

Section 1 Agenda

Section 1 will cover the concepts and principles of process related risk management, and the frameworks of Major Accident Prevention Policies and Safety Management Systems.

The concepts of process safety and functional safety and the requirements for process safety management and legislation will be covered. This section will provide an introduction to IEC 61511 for the Process Industries sector and the Safety Lifecycle and start to cover the PH&RA methods and inherently safe designs.

Content:

- Occupational Safety versus Process Safety;
- Risk management principles;
- Hazards and associated risks;
- Outline of EU SEVESO 2 Directive;
- Process Safety and Management Systems;
- Safety Legislation and Compliance;
- The ALARP concept;
- EC 61511 for the Process Industries;
- Management of Functional Safety;
- Prescriptive and Risk Based Standards;
- Inherent Safety;
- Process Lifecycle & Introduction to PH&RA Methods;
- Safety Instrumented Functions (SIF);
- Process Risk and Risk Judgement.

Section 2 Agenda

This section will cover the most common hazard identification methods including What IF and Hazard and Operability (HAZOP) Studies in line with IEC 61882. The concepts of Cyber Process Hazard Analysis will be introduced as well as the Bowtie method for linking hazards to process safety management (PSM). This section will also cover Failure Modes and Effect Analysis (FMEA) for identifying the effects of single equipment and system failures on systems or process plant.

Content:

- Hazard Identification Methods;
- HAZOP Guide IEC 61882:

    - Definition of scope and objectives of a HAZOP study
    - HAZOP Methodology
    - Preparatory work and documentation requirements;
    - Choosing the team and understanding roles within the team;
    - Understanding the role of the Team Leader;
    - Choosing Nodes;
    - The examination by guidewords, parameters and deviations;
    - The HAZOP study procedure;
    - Raising actions and action management;
    - Documentation and reporting of a HAZOP study plus formulating the study report;
    - Estimating HAZOP study duration;
    - Life cycle phases of HAZOP Study.
- HAZOP exercise;
- What-If Analysis;
- Checklist Analysis;
- What-If / Checklist Analysis;
- Bowtie method;
- HAZOP or What-If of non-routine operating modes;
- Failure Modes and Effect Analysis.

Section 3 Agenda

Section 3 will introduce the concept of how SIS can provide Primary and Secondary Functions for protection against different types of hazards. It will cover a number of alternative and popular methods for risk assessment techniques and will discuss the relationships between different methods and where they can be employed to best effect. The requirements for the Safety Requirements Specifications (SRS) and its development will be discussed in detail.

Content:

- Primary and Secondary Functions;
- Qualitative method of risk analysis:
    - The risk graph;
    - Risk graph calibration.
- Layer of Protection Analysis – semi quantified analysis:
    - Analysis of hazards by causes and event frequencies;
    - Independent protection layers (IPL);
    - Layers of protection;
    - Mitigation layers;
    - Conditional modifiers;
    - Setting tolerable risks for safety, asset and environmental consequences;
    - The LOPA analysis.
- Event Tree Analysis (ETA) – semi quantified analysis:
    - ETA Barriers and protection layers;
    - Qualitative ETA;
    - Event tree construction;
    - Quantified ETA;
- Fault Tree Analysis (FTA) – fully quantified analysis:
    - Functions of ‘AND’ and ‘OR’ gates;
    - Fault Tree rules;
    - FTA construction.
- Safety Requirements Specification (SRS).

The workshop will use numerous practical examples and team exercises to stimulate a realistic hazard and risk assessment experience.

Examination on Day 5

A five (5) hour two part proficiency assessment comprising:

Part 1 = 70 multiple choice questions (1 mark each question);
Part 2 = Two written question as follows:

Part 2.1 SIL determination question (12 marks);

Part 2.2 HAZOP question (18 marks).

The pass score criterion is 75%.

TÜV Rheinland Functional Safety Technician Certificate Training (4 days)

General information about this training

This 4 day course is not simply a watered down version of the FS Engineer course. It has been specifically designed to cater for the needs of Technicians by Engineers who have had significant technician experience in their own career development. The FS Technician (TÜV Rheinland) certificate course is run in accordance with the TÜV Rheinland Functional Safety Training Program and comprises three days of classroom tuition and practical guidance, for understanding and mastering lifecycle phases for testing, maintenance and change control of safety instrumented systems in accordance with the requirements of IEC 61508 / IEC 61511. There is a 2 part competency examination on the fourth day. Practical exercises will performed throughout the course which will be based on real life examples.

The examination on the last day comprises:

1. Multiple choice questions (60 marks available)
2. Open written questions (40 marks available)

The pass score requirement is 75 %.

Course objectives

The objectives of this course are to provide participants with a basic understanding of hazards and risk and how safety instrumented systems are used to protect against hazards. The main lifecycle focus will be on the principles of installation commissioning and maintenance, techniques. Guidance will be given on achieving good practice testing of the most common types of SIS subsystems. They will learn how testing and maintenance should be recorded to enable better reliability analysis of hardware components used in SIS subsystems, and how an optimised testing and maintenance regime improves plant safety and availability.

Throughout the course, emphasis will be placed on experience and realistic practical exercises, and case studies will be used to compliment the instruction.
Successful participants, who also have sufficient experience as a Technician working in the area of Functional Safety and SIS, will be awarded the prestigious FS Technician (TÜV Rheinland) certificate.

The course will provide 3 days of classroom tuition and practical guidance, mixed with exercises based on real life examples. This will be followed by a two part 3 hour proficiency examination on day 4.

Who should attend?

Technicians involved in the installation, development and/or maintenance support of electrical, electronic and programmable electronic Safety Instrumented Systems (E/E/PES) for process plant applications.

Eligibility requirements

In accordance with the TÜV Rheinland Functional Safety Training Program:

- Technicians working with Safety Instrumented Systems for a minimum of 2 years;
- Completed TÜV Rheinland Eligibility form;
- Qualification with a National Certificate, or equivalent, in a relevant technician discipline, or reference letter from employer.

Certificate

Successful participants, who must also have a minimum of 2 years of experience in the installation, development and/or maintenance support of electrical, electronic and programmable electronic Safety Instrumented Systems (E/E/PES) for process plant applications, will achieve the prestigious FS Technician (TÜV Rheinland) certificate. All FS Technicians of the TÜV Rheinland Functional Safety Training Program are also listed on the TÜV Rheinland Certipedia Database: www.certipedia.com.

Day 1 and the Morning of Day 2

Objectives:
This section is intended to give participants an understanding of Functional Safety in line with the international IEC 61508 and IEC 61511 standards, and the role of Safety Instrumented Systems (SIS) in reducing process related risk. They will be given a basic introduction to risk assessment so that they understand how Safety Integrity Levels (SIL) are established for SIS and how the SIL relates to risk reduction. The basic concepts of SIS subsystem design will be discussed to give an appreciation of how this is related to the SIL.

Content:

- An Introduction to Functional Safety and the Safety Lifecycle;
- A brief overview of the IEC 61508 and IEC 61511 standards;
- The concept of process related hazards and associated risks;
- An overview of the approaches and objectives of risk assessment;
- Achieving risk reduction in line with ALARP principles;
- The role of Safety Instrumented Systems in risk reduction;
- The importance of testing and maintenance in Functional Safety Management;
- The basic concepts of SIS subsystem design;
- The relationships between SIS designs and testing requirements;
- Human factors and common cause failure issues.

The workshop will use numerous practical examples and team exercises drawn from real life experience to support understanding.

The Afternoon of Day 2 and Day 3

Objectives:
To give participants a firm understanding of the good practice principles of testing techniques and procedures for the most common types of SIS subsystems in line with the international IEC 61508 and IEC 61511 standards. To demonstrate how appropriate testing and maintenance is important to sustaining reliability. To learn how testing and maintenance should be recorded to enable better reliability analysis of hardware components used in SIS subsystems and how an optimised testing and maintenance regime improves plant safety and availability.

Content:

- SIS installation and commissioning;
- Overall SIS Validation;
- The Relationship between SIS testing, failures and reliability;
- Safe failure modes and dangerous failure modes;
- To understand and evaluate the effects of testing and maintenance on SIFs;
- Proof testing techniques for SIS, and associated operational constraints:
    - Proof testing practices for measurement subsystems;
    - Proof testing practices for final elements;
    - Content of proof testing procedures;
    - Format of proof testing procedures;
    - Planning and scheduling;
    - Proof test records.
- Partial closure testing of valves;
- Overrides;
- Authorisation;
- Alarms and Diagnostics;
- Modifications and management of change.

Day 4

A two part proficiency examination comprising:

- Part 1 - multiple choice questions;
- Part 2 - written questions.

The pass score criterion is 75% in both parts.

Benefits of this course

Participants will be taken through the good practice principles of testing for the most common types of SIS subsystems and shown how appropriate testing and maintenance is important to sustaining reliability.

They will learn how testing and maintenance should be recorded to enable better reliability analysis of hardware components used in SIS subsystems and how an optimised testing and maintenance regime improves plant safety and availability.

Duty holders will be able to demonstrate compliance with the relevant competence requirements of IEC 61508.

Introduction to Functional Safety and Safety Instrumented Systems (IEC 61508 & IEC 61511) (0.5 day or 1 day)

General information about this training

This workshop can be customised for a 0.5 day or 1 day duration and will take participants through the fundamental principles of IEC 61508 and IEC 61511. It will include the concept of process hazard analysis and SIL determination risk assessment with the main focus on the Layer of Protection Analysis (LOPA) method. Participants will also be given the basic principles of safety instrument system design and shown the importance of testing and maintenance of such systems. This is the ideal workshop for preparation for the Functional Safety Engineer courses.

Who should attend?

Process engineers, safety engineers, instrument engineers and operations people involved with maintaining the integrity of process plant, or with design, development and maintenance of safety instrumented systems for process plant protection.

The objectives of the workshop will cover:

- An overview of the safety lifecycle;
- An understanding of the concepts and objectives of process hazard analysis;
- An understanding of the concepts and objectives of risk assessment;
- The analysis of safety, asset and environmental risk;
- Qualitative and quantitative methods of risk assessment;
- An understanding of the ALARP principles;
- Setting tolerable risk targets;
- An overview of Risk Matrices;
- An overview of Risk Graphs;
- The principles of Layer of Protection Analysis (LOPA);
- Hands on experience with the LOPA risk assessment method;
- Calibration of LOPA risk assessment for different consequences;
- Analysis of cause events and likelihood data;
- Cause and consequence scenarios;
- Independent protection layers and associated rules;
- An understanding of the differences between risk prevention and risk mitigation;
- Assigning values to risk reduction layers;
- Safety, Asset and Environmental conditional modifiers;
- Avoiding common cause issues (double dipping);
- SIS design and development;
- The PFD calculation;
- An understanding of the effects of testing and maintenance on SIFs;
- To understand the impact of common cause failures;
- To be able to select and use appropriate reliability data.

The workshop will use numerous practical examples and team exercises drawn from real life experience to stimulate a realistic hazard and risk assessment experience. The LOPA methodology will be based on IEC 61511, and *'Layer of Protection Analysis Simplified Risk Analysis; American Institution of Chemical Engineering ISBN 0-8169-0811-7.*

SIL Determination Workshop (2 days)

General information about this training

This 2 day workshop is intended to take participants through the fundamental principles of process hazard identification (HAZID, HAZAN and HAZOP) and SIL determination risk assessment using such methods as Layer of Protection Analysis (LOPA), Risk Graphs and Fault Tree Analysis (FTA) in line with the international IEC 61508 and IEC 61511 standards.

Who should attend?

Process engineers, safety engineers and instrument engineers involved with maintaining the process safety, asset or environmental integrity of process plant, or with the development of safety instrumented systems for process plant protection.

The objectives of the workshop are to equip participants with:

- The concept of identifying process related hazards.
- Hazard analysis by causes, deviations and consequences.
- The use of the formal guideword and parameter techniques for hazard analysis.
- An understanding of the concept and objectives of risk assessment.
- The analysis of safety, asset and environmental risk.
- Qualitative and quantitative methods of risk assessment.
- An understanding of the differences between risk prevention and risk mitigation.
- An understanding of the ALARP principles.
- Setting tolerable risk targets
- Hands on experience with different risk assessment methods.
- Basic concepts of Fault Tree Analysis (FTA) for SIL determination.
- Risk graphs and risk matrices.
- Risk graph calibration.
- The principles of Layer of Protection Analysis (LOPA).
- Calibration of LOPA risk assessment for different consequences.
- Analysis of cause events and likelihood data.
- Cause and consequence scenarios.
- Independent protection layers and associated rules.
- An understanding of the differences between risk prevention and risk mitigation.
- Assigning values to risk reduction layers.
- Safety, Asset and environmental conditional modifiers.
- Avoiding common cause issues (double dipping).
- An ability to participate in LOPA risk assessments.

The workshop will use numerous practical examples and team exercises drawn from real life experience to stimulate a realistic hazard and risk assessment experience. The LOPA methodology will be based on *'Layer of Protection Analysis Simplified Risk Analysis; American Institution of Chemical Engineering ISBN 0-8169-0811-7.*

SIS Design and Development Workshop (2 days)

General information about this training

This 2 day workshop is intended to take participants through the factors that need to be considered when performing Safety Instrumented Systems (SIS) and Safety Instrumented Function (SIF) designs for low, high and continuous demand mode process sector related applications in line with the international IEC 61508 and IEC 61511 standards.

Who should attend?

Engineers and systems integrators involved in the development of safety requirements specifications (SRS) and the detailed design of SIS and SIF, including verification calculations for the probability of failure on demand (PFD), probability of dangerous failure per hour (PFH), safe failure fraction (SFF), hardware fault tolerance (HFT) and common cause failures (CCF).

The objectives of the workshop are:

- To develop the SIS safety requirements specification (SRS) and select appropriate devices to meet the requirements;
- Considerations for field elements (do's and don'ts);
- To implement an appropriate SIF design architecture to meet the SRS;
- To perform the PFD, safe failure fraction and hardware fault tolerance calculations;
- To perform PFH calculations for high and continuous demand systems;
- To understand and evaluate the effects of testing and maintenance on SIFs;
- To understand the impact of common cause failures;
- To be able to select and use appropriate reliability data.

It is focused on the design phase which is covered in considerable detail and includes the following topics:

- SIS Design and Development;
- Integrity Specification of a SIF;
- SIS Safety Requirements Specification;
- Selection of Components and Subsystems;
- Proven in Use;
- Field Devices;
- Failures;
- Failure and Reliability;
- Probability of Failure on Demand;
- Demand Modes;
- SIS Implementation (low, high and continuous demand modes);
- Importance of Testing;
- Importance of Maintenance;
- Fractional Dead Times;
- Common Cause Failures;
- Safe Failure Fraction;
- Hardware Fault Tolerance;
- Calculating the PFD for systems with diagnostics;
- Subsystem Safety Integrity;
- Improving the PFD - Partial Closure Testing;
- Calculating PFH for high and continuous demand systems;
- Reliability data.

Course instruction will be complimented with examples, demonstrations and exercises to equip participants with methods and tools for SIF/SIS design and development for meeting the appropriate IEC 61508/61511lifecycle requirements.

Alarm Systems Management Workshop (1 day)

General information about this training

Alarm systems all too often suffer a proliferation of alarms that are both badly configured and incorrectly prioritised. They invariably contain far too many useless alarms which cloud the visibility of an operator. Poor alarm configuration leads to poor operator response with the consequences of excessive loss of production as a minimum and a significant probability of a loss of plant integrity.

This Alarm Systems Management Workshop will provide an introduction to alarm systems based on the EEMUA Publication 191: 'Alarm Systems - A Guide to Design, Management and Procurement'.

Who should attend?

Engineers involved in the configuration of alarm systems in the process control and emergency shutdown environments.

Objectives

The workshop will cover alarm system philosophy, the principles of alarm system design, procurement and implementation. It will also cover alarm performance metrics and the structure for managing and implementing an alarm improvement programme. Exercises will be used to enhance understanding and these are based on examples taken from practical experience.

The course content includes:

- What represents an alarm system;
- The role of the operator;
- The key design principles;
- What to alarm;
- Types of alarm;
- Risk assessment;
- Risk reduction;
- The selection of alarm settings;
- Alarm prioritisation;
- Reliability;
- Operability;
- Prioritisation;
- Implementation issues;
- Alarm displays and audible warnings;
- Training;
- Testing;
- Measuring performance;
- Managing an improvement programme;
- Alarm system procurement;
- EXERCISES.

Layer of Protection Analysis Workshop (1 day)

General information about this training

This 1 day workshop is intended to take students through the fundamental principles of performing Layer of Protection Analysis (LOPA). It will provide clear guidance on Independent Protective Layers (IPL) and the rules for determining the 'independence of different' layers. Active, passive and procedural protective layers will be examined along with the required rules for taking credit for any risk reduction measure.

The rules for taking credit for basic process control systems (BPCS) loops will be explained along with taking credit for multiple BPCS loops. Examples of how to BPCS loops should be physically connected to form IPLs will also be provided.

The maintenance requirements for any IPL to comply with dependability rules will be covered.

The IEC 61511 Edition 2 - 10,000 times risk reduction limitations for instrumented layers will be thoroughly explained along and examples provided.

Who should attend?

Engineers involved in safety integrity level (SIL) determination for risk assessment of safety instrumented functions.

The objectives of the workshop are to equip participants with:

- An understanding of the concept and objectives of risk assessment;
- An understanding of the concept and objectives of risk reduction;
- An understanding of the ALARP principles;
- An understanding of the differences between risk prevention and risk mitigation;
- An understanding of the principles of LOPA;
- Independent Protection Layers (IPL);
- Rules for taking credit for IPLs;
- Basic Process Control System (BPCS) layers;
- Avoidance of risk reduction "double dipping";
- Scenario based consequence severities;
- Target Mitigated Event Likelihood (TMEL);
- Consequence equivalence tables;
- Prevention layers;
- Mitigation Layers;
- Conditional Modifiers;
- Limitations on instrumented layers of protection;
- The opportunity to participate in very practical LOPA risk assessment examples.

The workshop will use a number of practical LOPA examples and team exercises to stimulate a realistic risk assessment experience. The methodology will be based on *the international standards IEC 61508 and IEC 61511 and 'Layer of Protection Analysis Simplified Risk Analysis; American Institution of Chemical Engineering ISBN 0-8169-0811-7.*

TÜV Rheinland Cyber Security Program – Security Risk Assessment Training (4 days)

General information about this training

This 4 day Cyber Security Risk Assessment (TÜV Rheinland) course is run in accordance with the TÜV Rheinland Cyber Security Program and comprises of three days of classroom tuition and practical guidance to provide evidence of competency with respect to assessing and specifying Industrial Automation Control System (IACS) security.
Successful participants, who have sufficient experience and pass both the fundamentals and Security Risk Assessment exam, will be eligible for the prestigious CySec Specialist (TÜV Rheinland) certificate in Security Risk Assessment.

Course objectives

The objectives of the course are 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

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 four-hour two-part examination based on a multiple choice and an Open SRA examination.

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 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.

Certificate

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

Day 1 Agenda

Day 1 provides the 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: IEC61511 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 prioritizes 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 four (4) hour two-part competency examination comprising:

- Part 1 = 30 multiple choice questions (1 mark each question);
- Part 2 = Open examination with 7 questions (10 marks each question)

The pass score criterion is 75%

The benefits of selecting C&C for your training needs:

C&C have over 50 years of Oil and Gas related processing experience and all our Functional Safety consultants and trainers are TÜV Rheinland Functional Safety Experts. C&C are globally recognised for their Functional Safety expertise and our Engineers have chaired numerous committees and panels associated with this area of engineering. We have been contracted to undertake many Functional Safety Assessments for onshore and offshore related projects for numerous UK based operators.

C&C have been selected as the approved training organisation for the provision of Functional Safety related training by Aker, BP, ConocoPhillips, Chrysaor, EnQuest, Baker, GE, Fluor, INEOS, KPC, Lloyds, Maersk, National Grid, Petrofac, Petronas, QAPCO, SABIC, Shell UK, Spirit Energy, TOTAL, Wood Group PSN, Worley and many other globally based duty holders. Companies such as BP, Shell UK, Total and Wood Group PSN put all their staff engineers through the C&C FS Engineer training.

C&C is one of the leading providers of the TÜV Rheinland FS Engineer training program having successfully trained over 2,000 FS Engineers (TÜV Rheinland) fir SIS and PH&RA, with a success rate of around 95%.

TÜV Rheinland Functional Safety Experts and Approved Trainers
All training will be undertaken by TÜV Rheinland Functional Safety Experts who have been approved by TÜV Rheinland to provide their training programs.

Training Fees
These are based on a per delegate basis and will vary by location and participant numbers. Large training groups will enjoy significant discounts, and C&C will be pleased to provide a quotation to meet your training requirements on request.

Location and Facilities
The training location and facilities, including power beam projection, flipcharts and stationary can be provided by the client or arranged by C&C at additional cost.

Training Attendance
We recommend group training sessions as these will facilitate stimulating discussion for exercise purposes. C&C can provide training on a one-to-one basis but our daily rate consultancy fees will apply.

Training Manuals
Training manuals containing all the presented material and exercise examples will be provided for each student.

Contact Details

C&C Technical Support Services

T: + 44 (0) 13398 86618
F: + 44 (0) 13398 85637
E: info@silsupport.com
W: www.silsupport.com