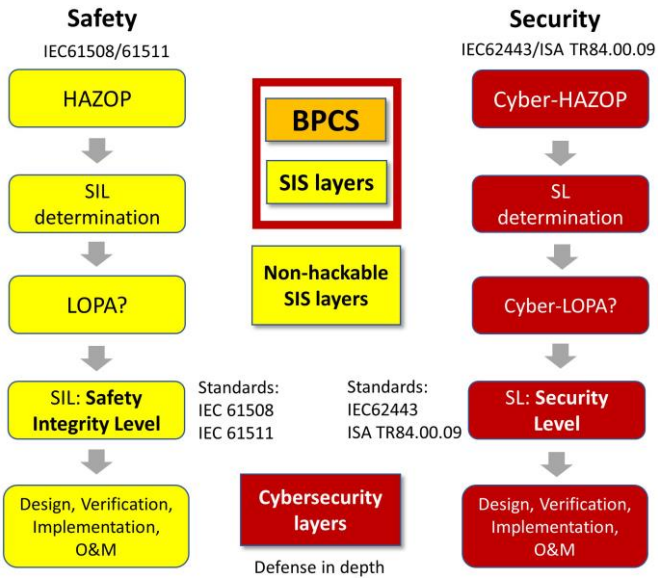
Training on Functional Safety

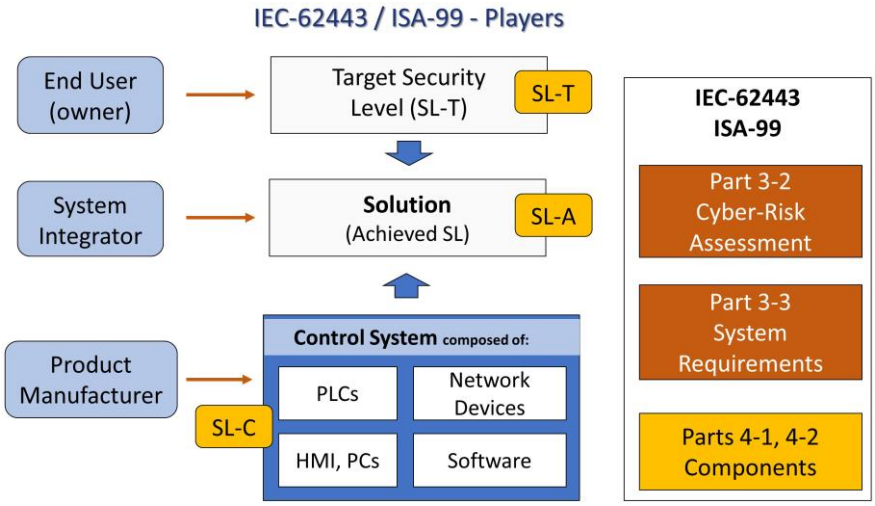
safetyandsis.com

Course 3

Cyber-HAZOP/LOPA Analysis

- Based on ISA Technical Report "TR84.00.09-2017", and the Standards IEC 62443, IEC61511/61508.
- The course is structured in 6 modules: Risk Concepts, IEC62443 vs IEC61511, Methodologies, Practical Examples, Practical Exercise, Security Level Verification.
- Duration: 8 hours with MS-Teams.
- Virtual instructor-led training (VILT) at the time agreed with the participants.





Clause 11.2.12 of IEC 61511:2016:

"The design of the SIS shall be such that it provides the necessary resilience against the identified security risks (see 8.2.4).

Note: Guidance related to SIS security is provided in ISA TR84.00.09 and IEC 62443-2-1:2010".

Other available courses:

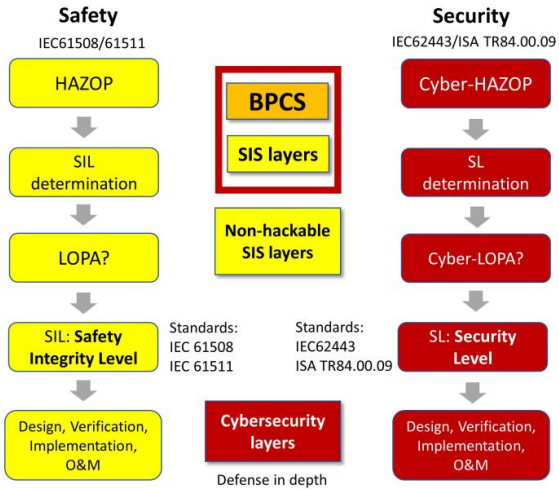
Course 1: Functional Safety & Safety Instrumented System (SIS)

Course 2: Design of SIFs & SIL Verification

The complete functional safety training program consists of three training courses. Our instructors have a lot of training experience in collaboration with ISA, TÜV Rheinland and TÜV SÜD.

Training on Functional Safety

Cyber HAZOP/LOPA Analysis



Cybersecurity Risk Analysis with methodologies Cyber-HAZOP & Cyber-LOPA. The course is structured in 6 modules:

- ✓ **Risk Concepts**
- ✓ **IEC 62443 vs IEC 61511.**
- ✓ **Methodologies.**
- ✓ **Practical examples.**
- ✓ **Practical exercise.**
- ✓ **Verification of SL.**

Aimed at

The course is especially aimed at **HAZOP-LOPA technicians** in the process industry due to the need to incorporate the cybersecurity analysis required in IEC 61511 (clauses 8.2.4 and 11.2.12). **No knowledge of cybersecurity is required**. The course is also of interest to **cybersecurity technicians** from the IT world who will be involved in cybersecurity risk analysis in the OT world.

Course objetive

The objective is to learn **how to perform cybersecurity risk analysis** from the traditional IEC 61511 risk analysis. The Cyber-HAZOP can be performed at the same time or after the HAZOP analysis, taking advantage of the scenarios identified in the "Hazard and operability" analyses.

Course Methodology

-Course in english.

-Approximate duration: 8 hours.

-Methodology: based mainly on real examples and practical exercises. An Excel tool specifically designed for this course is used.

-Participants take part in the examples and exercises of the course, as well as answer the online tests carried out during the course.

Documentation

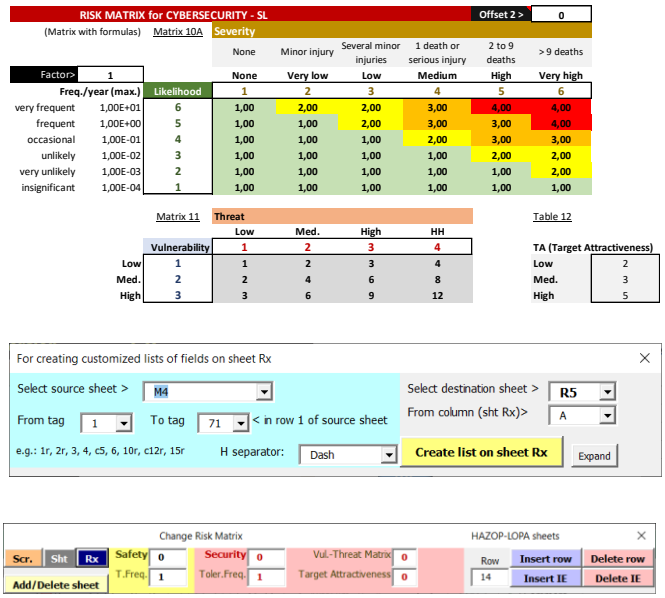
Course contents in PDF format.

Certificate of the course completion.

Excel Tool

Excel file: HAZOP, Calibrated Risk Graph, Risk Matrices (safety & security), Probability, Cyber-HAZOP, LOPA and Cyber-LOPA. Examples and solved exercises (high level assessment, detailed assessment, SL verification).

More info



Contents of the course

Module 1: Risk Concepts

-How risk is quantified, examples in "safety" and "security".

-Risk Gap, Tolerable Risk, Layers of protection.

-The risk matrices used in the course (safety & security)

Approx. duration: 60 minutes

Module 2: IEC 62443 vs IEC 61511

-Similarities in life cycle of both standards.

-Concepts: SIF, SIL, SIS, Security Levels (SL).

-IEC62443: High-level analysis, detailed analysis, Zones and Conduits.

-Vulnerabilities: Assessment, public databases, life cycle, examples, etc.

-Threats: Sources, attack vectors, etc.

Approx. duration: 90 minutes

Module 3: Methodologies

-Explanation of the Excel tool of the course.

-Basic example of HAZOP and LOPA (for non-HAZOP experts).

-Cybersecurity Risk Analysis: Methodologies proposed in ISA TR84.00.09, consequence-driven method (SPR), assessment with probability, advantages and limitations of each method, examples.

Approx. duration: 90 minutes

Module 4: Practical examples

-Explanation of the case study (industrial process).

-Result of HAZOP/LOPA with Excel tool.

-High level Cyber HAZOP: a)Advantages of SPR method; b)Use of probability; c)Calculation of required SL; d)Non-hackable layers; e)Examples of the impact of changing the risk matrix and how to calculate probability.

-Cyber LOPA: Calculation of CRRF and required SL and other considerations.

Approx. duration: 90 minutes

Module 5: Practical exercise

-Explanation of the case study.

-Assignment of parts of the exercise to course participants.

-Sharing of the CyberHAZOP-CyberLOPA results.

Approx. duration: 90 minutes

Module 6: Verification of Security Level

-IEC 62443 requirements (foundational and system requirements).

-Example of a detailed Cyber Risk Analysis.

-Examples of Security Level Verification.

Approx. duration: 60 minutes

Addtional information in the website