MCL CONTROL

Functional Safety in Processes, Risk Analysis and Safety Instrumented Systems

Part II: Specifications of the Security requirements of a SIS. Conceptual design of the SIS and SIL verification.

A.- General objectives

1. Expand practical knowledge in the application of Safety Instrumented Systems (SIS) in the process industry.
2. Specify the Security Requirements of a SIS.
3. Propose the conceptual design of the SIS, to comply with the SRS.
4. Understand the SIL Verification process of a SIS.

B.- Competences to develop.

1. Specify the security requirements of a SIS.
2. Define and evaluate the configuration of the Safety Instrumented Functions (SIF) to achieve the required SIL.
3. Apply the security life cycle to a SIS in industrial process plants.

C.- Addressed to:

Instrumentation and control engineers and technicians dedicated to the specification, design, implementation, operation and maintenance of Safety Instrumented Systems. System integrators. Systems consultants. Plant engineers and technicians. Engineers and supervisors in charge of electrical plant maintenance. Process control engineers. Engineers who want to prepare for the functional safety certification exam.

D.- Methodology:

- "Online" modality course with sessions recorded and available to be reviewed later.
- Theoretical / practical – Exercise sessions.

E.- Previous knowledge

General knowledge of industrial instrumentation and automatic control systems. Basic knowledge of electrical engineering principles. Engineering studies or equivalent, related to the area in question. have completed.

F.-Content

Chapter 1.- Specifying the security requirements (SRS) of a SIS.

Development of general security requirements. Development of the SRS. Documenting the SRS.

Chapter 2.- Selection of technologies and the conceptual design stage.

What is required by the standards? The conceptual design phase according to the ISA: “The grandfather clause”. The conceptual design phase according to IEC. Logic Solver technologies. security PLCs. Classification and certification. SIS architectures.

Chapter 3.- Basic reliability analysis applied to SIL verification and safety instrumented systems.

Design objectives. The design process. Failure modes. Reliability formulas. Models and methods of analysis. Design considerations. Reliability calculation packages and databases. LIS verification. Fake shots.

Chapter 4.- Field devices and instrumentation

Field devices for safety. Sensor types. Guidelines for the application of field devices. Design requirements for field devices.

Chapter 5.- Engineering a security system: Hardware

Management and Engineering of security projects. Limitations to the SIS architecture. Detailed design of the SIS. Information flow and documentation in the engineering phase.

Chapter 6.- The application software.

Software problems. Fundamentals of the software life cycle. Steps for application software development.

Chapter 7.- Planning: Phases 6, 7 and 8 of the IEC

Benefits of planning in the design phase. Planning of maintenance and la operación. Planificaciónvalidation activities. Installation planning and commissioning.

Chapter 8.- Installation and commissioning (IEC phase 12)

Activity flow. Factory tests. Facility.

Chapter 9.- Validation, Operation and change management. (IEC phases 13, 14 and 15)

Verification, validation, and audit. Operation, maintenance and repair. Functional testing. Change management.

Chapter 10.- Justification of Safety Instrumented Systems.

Impact of SIS failures. Justification.

F.-Required tools

Scientific calculator.

G.-Duration

5 days in sessions of 4 hours each day.