



SERIES 1 – GETTING STARTED

Module 1 SIS Standards Overview

This course begins with a brief introduction to the various good engineering practices that apply to safety instrumented systems (SISs) implemented in process industry facilities. Special focus is given to international standards, such as IEC 61511 and 61508, and recognized guidance documents, such as the CCPS Guidelines books and several ISA technical reports.

Module 2 Existing SISs and the Lifecycle

Demonstrating the required integrity is an important part of proving safe operation. The US version of IEC 61511, ANSI/ISA 84.00.01-2004, contains Clause 1 y, which is known as the grandfather clause because it addresses SISs installed prior to the release of the standard. ISA TR84.00.04 provides guidance on assessing existing systems for compliance with the grandfather clause.

Module 3 Planning

A safety management system is required in IEC 61511 Clauses 5 through 7. Key management system elements are competence, independent review, verification, functional assessment, management of change, and auditing.

SERIES 2 – RISK ASSESSMENT

Module 4 Process Risk and Protection Layers

Process risk derives from process miss-operation and is an inherent part of process design. This inherent risk must be reduced below internationally accepted risk criteria using independent protection layers that are designed and managed to meet seven (7) core attributes.

Module 5 Establishing Risk Evaluation Criteria

The risk assessment phase should address the major requirements of IEC 61511 Clauses 8 and 9. The initiating events for process hazards are identified and the frequency of each potential event is determined. The consequence severity is defined for the process hazard assuming no steps are taken to stop the event. Various conditional modifiers may also be considered to offset risk in some types of analysis.

Module 6 Layer of Protection Analysis

Layers of protection analysis (LOPA) identifies the initiating events and their frequency, the consequences and their severity, the required risk reduction, and the protective functions implemented in each protection layer to meet the required risk reduction. A LOPA example will be presented.

SERIES 3 – DESIGN AND IMPLEMENTATION

Module 7 Process Requirements Specification

The process requirements specification provides the information required to define the instrumentation and controls used to implement SISs. Process engineering with input from operations personnel defines the requirements necessary to achieve the functionality, integrity, reliability, operability, and maintainability.

Module 8 Safety Requirements Specification

The Safety Requirements Specification (SRS) in IEC 61511 Clause 10 is a collection of information that defines the SIS design basis, which can be tailored to meet user needs. The standard also provides specific fault tolerance and separation requirements, which must be addressed during the physical allocation of the functions to the systems.

Module 9 Selection of Devices

SIS device selection is addressed in IEC 61511 Clause 11.5. ISA TR84.04 guidance is presented related to field devices and logic solvers. Emphasis is placed on demonstrating that the device is user-approved for safety based on manufacturer compliance information and actual field experience.

Module 10 Software Specification

Software performance is largely affected by systematic errors, i.e., mistakes made during software programming. IEC 61511 Clause 12 focuses on the development of application programs using limited variability languages and follows a lifecycle approach covering specification, verification and validation.

SERIES 4 – METRICS AND THE OPERATING BASIS

Module 11 Data Estimation

Performance verification includes the assessment of the probability of failure on demand (PFD) and the spurious trip rate of the SIS as specified and maintained. Various types of data estimates are discussed with an emphasis on collecting internal and industrial data.

Module 12 Design Decisions

The voting architecture, diagnostic coverage, proof test interval, and common cause failure potential affect the PFD and the spurious trip rate. The impact of each is discussed and typical examples are presented.

Module 13 Example Verification

A series of cases illustrate how choices in field device architecture, testing interval, and logic solver technology can affect the PFD and spurious trip rate.

Module 14 Operating Basis

There are many day-to-day operation and maintenance activities that must take place for the SIF to achieve its expected performance. Many operation and maintenance procedures must be written and verified prior to the introduction of hazards into the process unit. These procedures support the detection and response to faults and process alarms, the initiation of manual shutdown, reset after shutdown, and proof tests.