DAY 1 – GETTING STARTED

Module 1 SIS Standards Overview

The 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 Planning

An overview of IEC 61511 is presented followed by detailed requirements for the safety management system contained in Clauses 5 through 7. Key elements are competence, independent review, verification, functional assessment, management of change, and auditing.

Module 3 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 (IPLs) that are designed and managed to meet seven (7) core attributes.

Module 4 Establishing Risk Evaluation Criteria

The risk assessment phase is addressed in IEC 61511 Clauses 8 and 9. The initiating events for process hazards are identified and the frequency and consequence severity of each potential event is estimated. Depending on the type of risk analysis, various conditional modifiers may also be considered when assessing the risk. Once the risk is understood, a risk reduction strategy can be developed.

DAY 2 – RISK ANALYSIS TO DESIGN

Module 5 Layer of Protection Analysis

Layer of protection analysis (LOPA) is covered in the CCPS book, Layer of Protection Analysis: Simplified Process Risk Assessment. 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 achieve the required risk reduction.

Module 6 Safety Requirements Specification (SRS) Part 1

The SRS in IEC 61511 Clause 10 is a collection of information that specifies the SIS design basis required to ensure process safety during all operating modes. The SRS defines the functionality, integrity, reliability, operability, and maintainability requirements based on operational goals, intended operating modes and process safety time limitations.

Module 7 Safety Requirements Specification Part 2

IEC 61511 Clause 11 provides many specific design requirements including the need for fault tolerance and separation of the SIS from the BPCS.

Module 8 Selection of Devices

SIS device selection is addressed in IEC 61511 Clause 11.5. ISA TR84.00.04 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 a review of manufacturer information and actual field experience.

DAY 3 – VERIFICATION AND OPERATING BASIS

Module 9 Data Estimation

IEC 61511 Clause 11.9 requires verification of the SIS performance through calculation 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 10 Design Decisions

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

Module 11 Example Verification

An example SIF will be assessed to illustrate how choices in field device architecture, test interval, and logic solver technology affect the achievable PFD and spurious trip rate.

Module 12 Operating Basis

There are many day-to-day operation and maintenance activities that must take place for the SIS to sustain its expected performance throughout its installed life. Operation and maintenance procedures must be developed 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.