



- ✓ *4 Topical series offered in 14 on-line modules or in a 3-day class format*
  - *\$900 when purchased as package*
- ✓ *Test score of 80% is required to receive PRISM Certification.*

### **SERIES 1 – GETTING STARTED**

#### ***Module 1 Introduction to the SIS Standards***

Your introduction to IEC 61511 begins with a brief introduction to the importance of good engineering practices in meeting national process safety regulations. The current status of the good engineering practices for safety instrumented systems (SIS) is presented. Then, the relationship between IEC 61508 and IEC 61511 and the scope limitations of IEC 61511 are presented to set the foundation for a clause by clause overview of IEC 61511.

#### ***Module 2 The Grandfather Clause***

The Grandfather Clause is ANSI/ISA 84.01-2004 (IEC 61511 modified) Clause 1y. It addresses SISs installed prior to the release of the standard in 2004. OSHA citations related to the grandfather clause can be reviewed to establish the regulatory expectations for existing SISs. ISA TR84.04 Clause 3.0 and Annex A provide guidance on the Grandfather Clause.

#### ***Module 3 The Protective Management System***

The protective management system is covered in IEC 61511 Clauses 5 through 7. Key issues associated with management system are competence, independent review, verification, functional assessment, configuration management, and auditing.

### **SERIES 2 – RISK ASSESSMENT**

#### ***Module 4 Process Risk and Protection Layers***

Process risk has its origin in the process with the process demands and consequence. Process risk must be reduced to the owner/operator risk criteria. Various industrial risk criteria are available. Protection layers are used to reduce the process risk to the tolerable risk. These protection layers are designed and managed to meet seven (7) core attributes.

#### ***Module 5 Establishing H&RA Criteria***

The hazard and risk analysis (H&RA) phase must cover the major requirements of IEC 61511 Clauses 8 and 9. The initiating events for process hazards are identified and the frequency of the potential event is determined. The consequence severity is defined for the process hazard assuming no steps are taken to stop the event. Owner/operator risk criteria must be established to relate the initiating event frequency and the consequence severity to specific target risk reduction factors. Then, protection functions are identified and allocated to protection layers that can provide the required risk reduction.

#### ***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.

### **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 in IEC 61511 Clause 10 is a collection of information that yields the SIS design basis. The process requirements provide the SIS boundary and the constraints that are placed on each SIF. The focus of the design is achieving the required performance at the best lifecycle cost.

### **Module 9     *Selection of Devices***

How to properly select SIS devices per IEC 61511 Clause 11.5 is probably the number one area where the popular media is riddled with misrepresentation of the standard's actual intent. 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; a concept that has been around since the CCPS book Safe Automation. This uses manufacturer compliance information and actual field experience to choose a device that yields the required performance.

### **Module 10    *Software Specification***

Software performance is largely related to systematic errors, i.e., mistakes made during the programming of the software. IEC 61511 Clause 12 focuses on the development of application software using limited variability languages. A lifecycle approach is used with specification, verification and validation steps shown specifically for the software.

## **SERIES 4 – METRICS AND THE OPERATING BASIS**

### **Module 11    *Verification Fundamentals***

Performance verification includes the assessment of the probability to fail on demand (for demand mode SIFs) and the spurious trip rate. Design choices, such as inherent device integrity and reliability, voting architecture, diagnostic coverage, proof test interval, and common cause failure, affect the SIF probability to fail on demand and the spurious trip rate.

### **Module 12    *Data Decisions***

IEC 61511 Clause 11 uses the performance expectations to drive the design and management of the SIS hardware. Various data decisions must be made with regard to the failure rate data, diagnostic coverage, mean time to repair, and common cause failure. Comparison of device data illustrates the wide variance in performance across technologies.

### **Module 13    *Example Verification***

A series of cases illustrate how choices in field device architecture, testing interval, and logic solver technology can affect the probability to fail on demand. Partial stroke testing of block valves will also be illustrated.

### **Module 14    *Operating Basis***

Designing a good SIF is only half the battle in achieving safe operation. The other half is the day-to-day operation and maintenance practices 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.