SIS 103 - Safety Standards

15 minutes

In this course:

Overview

If your plant or process isn't already using safety standards such as IEC 61508, IEC 61511, and/or ANSI/ISA S84.00.01-2004, chances are you will be in the near future.

Although you may initially think of them as sources of paperwork, hassles, and headaches, these standards play a vital role in making — and keeping — your plant safe. Their disciplined approach can also help ensure that your process control system, operational and maintenance procedures, and safety systems are harmonized in a way that leads to better operational performance.

This course introduces the most relevant safety standards — IEC 61508, IEC 61511, and ANSI/ISA S84.00.01-2004 — and explains why complying with them makes good business sense.

What do all those acronyms stand for?

IEC - International Electrotechnical Commission
ISA - The Instrumentation, Systems, and Automation Society
ANSI - American National Standards Institute

Hint

As you go through the topics in this course, pay special attention to the following:

- How safety standards have changed
- Which standard is your best choice for new safety applications
- The benefits of standards-based life-cycle models
- What kinds of resources are required for compliance
- The key benefits of compliance

A New Approach

In the past, safety standards were developed for a specific application, industry, or country. For example, ANSI P1.1-1969 is an industry consensus standard issued by the American National Standards Institute that defines safety requirements for mills producing pulp, paper, and paperboard.

The major problem with this approach is that plants, and even entire industries, have found themselves trying to comply with multiple, overlapping safety standards that were often developed using completely different design and architecture philosophies. Add in the nuances of country or regional standards, and being sure you've achieved compliance becomes nearly impossible.

Newer safety standards, however, have been developed using an approach that focuses on reducing risk and establishing a defined degree of operational excellence at each stage of the safety project's life cycle.

This performance-based **life-cycle** approach produces a standard that more easily meshes with other standards, thus creating broader appeal and acceptance. It also makes it easier to produce high-quality results at the least possible cost.

For process industries, the relevant safety standards are IEC 61508, IEC 61511, and ANSI/ISA S84.00.01-2004 (S84). These standards each define ***what*** is required to attain standard compliance, but in the case of IEC 61511 and S84 they leave the details of ***how*** to achieve compliance to plant owners and operators.

From IEC 61508 Came IEC 61511

So why does IEC have ***two*** safety standards?

IEC 61508 (Parts 1 - 7), titled *Functional safety of programmable electronic safety-related systems*, is a comprehensive, all-inclusive, performance-based functional safety standard that applies to manufacturers and implementers of functional safety systems in a broad range of industries.

In Europe, the seven parts of IEC 61508 are published as EN 61508, and any conflicting national CENELEC or CEN standards were subsequently withdrawn.

IEC 61508 was used by some process industry plants to implement compliant safety instrumented systems

(SIS). However, early process-industry adopters noted that the standard was cumbersome and left too much room for interpretation on how to achieve compliance in these industries.

After careful consideration, the IEC standards committee extracted, harmonized, and reworded relevant sections of IEC 61508 to form IEC 61511 specifically for process industries.

The result is that IEC 61511 provides the process industries guidance and examples of how the standard is implemented -- while still ensuring compliance is achieved within the framework set forth in IEC 61508.

This approach has made IEC 61511, *Functional safety: Safety instrumented systems for the process industry sector*, the safety standard of choice for process industries — as witnessed by the growing number of references to it by safety agencies in China, Ireland, Italy, India, Norway, United Kingdom, and the United States; the number of papers being presented by end-users at conferences and symposiums; and the references on control system manufacturers' Web sites.

While plants still have the option of applying IEC 61508, its main use is by instrumentation and control system manufacturers developing and selling SIS certified devices for use in IEC 61511-compliant applications.

What About S84?

Many national standards have been superseded by IEC 61508 and 61511. One example is the ANSI/ISA S84.01 safety standard that was widely used in the United States.

Several years ago, following a number of unnerving accidents, safety experts within the process industry began a thorough review of existing safety standards.

Incidents leading to improved safety standards		
1968	Pernis oil refinery, the Netherlands	2 dead, 85 injured
1974	Flixborough, United Kingdom	28 dead, hundreds injured
1976	Seveso, Italy	700 injured
1984	Bhopal, India	2,500 dead, 100,000 injured
1998	Piper Alpha, North Sea	165 dead, 61 injured

Among their conclusions was that existing standards were too industry-specific and limited the ability of safety experts to share best practices.

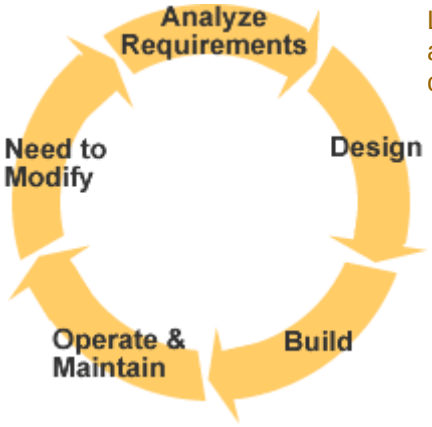
From those findings came the formation of the ISA SP84 committee. Almost immediately, committee members agreed that a more appropriate standards approach would be to use a performance-based life-cycle model. The result of their work was ANSI/ISA S84.01-1996, *Application of Safety Instrumented Systems for the Process Industries* (S84).

More recently, however, the S84 standard has been harmonized with IEC 61511, with one exception: ANSI/ISA S84.00.01-2004 includes a "grandfather" clause allowing installations currently using the 1996 version of S84 to continue doing so — provided they determine that the safety equipment is designed, maintained, inspected, tested, and operated in a safe manner.

Unless you're already using S84, therefore, your best choice would be to forgo the old ANSI/ISA standard and adopt IEC 61511 — which is the same as S84-2004.

Life-cycle Models

A life-cycle model provides a structure for a series of processes to create or update a product or service.



Life-cycle models can take many forms, but each provides a structure for approaching the myriad tasks involved in creating and managing a complex product or service.

A major benefit of a life-cycle-based standard is the ease it provides to leverage and integrate other life-cycle-based standards and practices. As the table shows, such models are used or recommended by a number of regulatory agencies and other bodies.

Organizations & agencies recommending use of life-cycle models	
International Standards Organization (ISO)	Product & service quality
U.K. Health & Safety Executive	Safety-related activities
U.S. Food & Drug Administration	New drug approval and production
Software Engineering Institute	High-availability software
U.S. Occupational Safety & Health Administration	Worker safety
U.S. Environmental Protection Agency	Environmental protection

For example, the Software Engineering Institute has developed a number of software life-cycle models, several of which are used to create "survivable" software — that is, mission-critical application software requiring security, fault tolerance, safety, reliability, reuse, performance, verification, and testing.

Similarly, life-cycle-based current Good Manufacturing Practices (cGMPs) are integral to industries where product quality is essential, like those regulated by the U.S. Food & Drug Administration.

Besides making it easier to integrate such standards, the discipline provided by the life-cycle approach helps produce high-quality results at the least possible cost.

Applying the Model in 61511

IEC 61511 permits customizing the life cycle model to fit your current practices - as long as you meet the standard's requirements.

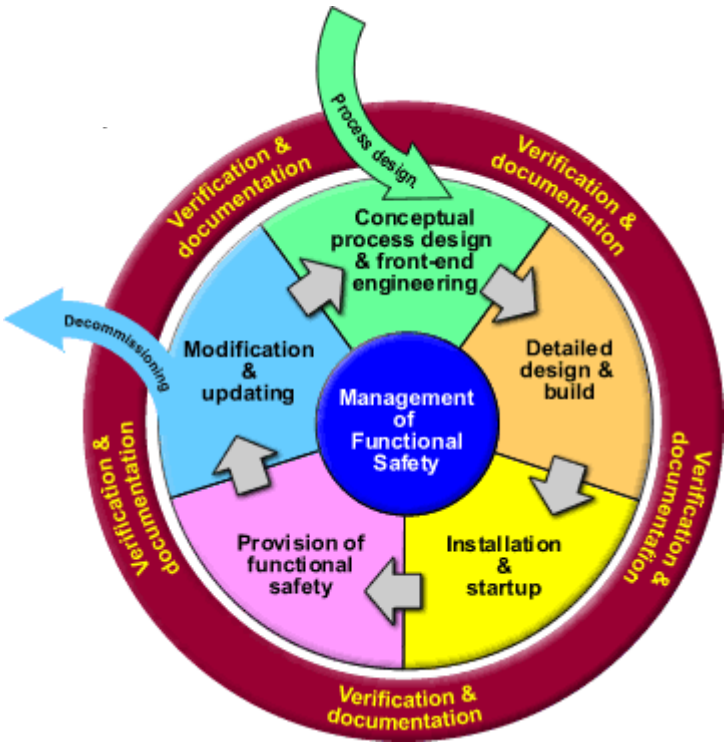
One approach uses five major life-cycle stages to address these requirements, plus a verification and documentation process throughout the cycle:

Life-cycle stage	IEC 61511 requirements
1. Front-end engineering and conceptual design	Hazard and risk assessment (Clause 8) Allocation of safety functions to protection layers (Clause 9) Safety requirements specification for the SIS (Clauses 10 and 11)
2. Detailed design and engineering	SIS design and engineering (Clauses 11 and 12.4) SIS build, integration, and FAT (Clause 13)
3. Installation and startup	SIS installation and commissioning (Clause 14) SIS safety validation (Clauses 12.3, 12.7, and 15)
4. Provision of functional safety	SIS operations and maintenance (Clause 16)
5. Modification and updating	SIS modification (Clause 17)
- Verification and documentation (included in each stage)	Verification (Clauses 7, 12.4, and 12.7) Documentation (Clause 19)

Together, these activities add up to meet the core requirement of IEC 61511:

Management of functional safety	Management of functional safety and functional safety assessment and auditing (Clause 5) Safety life cycle structure (Clause 6.2)

The following diagram shows how these activities fit together.



Front-end engineering & conceptual design

- Create conceptual process design
- Identify potential hazards
- Allocate safety requirements
- Decide whether an SIS is required
- Identify levels of tolerable risk and select target SILs
- Create Safety Requirements Specification
- Select technology, architecture, and proof test philosophy
- Calculate SIL for each safety function

Detailed design

- Detailed design of
  - SIS field devices installation
  - SIS logic solvers hardware
  - SIS software
- Design verification
- Logic solver hardware build and verification
- SIS software configuration and safety function testing
- Integration of SIS logic solver
- Verification of integration (FAT)
- Create installation & commissioning documentation
- Create operations & maintenance documentation

Installation & startup

- Install SIS field devices
- Install SIS logic solvers
- Integrate SIS into BPCS as required
- Verify installation
- Commission SIS
- Validate SIS

Provision of functional safety

- Operate and maintain SIS in accordance with documented procedures
- Perform proof tests as defined in the design to verify operation of the SIS

Modification & updating

- Assess scope of modification
- If change does not affect safety case then make change, and complete all required verification and change management procedures
- If change is significant then repeat the Safety Lifecycle

Resources for Compliance

Obviously, saying your company is committed to providing a safe working environment isn't enough. Management has to provide the resources needed to fulfill that commitment – including appropriate funding, people, and training. That's part of building the environment and culture that must exist before IEC 61511 compliance can be achieved.

IEC 61511 requires having persons with demonstrated safety engineering knowledge and experience appropriate for the process and the SIS technologies being used. The standard also says that the people assigned to engineer, design, and implement safety systems must have

- adequate training,
- management and leadership skills appropriate to their role in safety life-cycle activities, and
- knowledge of the applicable legal and safety regulatory requirements.

It then becomes the job of these safety professionals to establish documented evidence that conformance to the IEC safety standard has been appropriately defined, achieved, and maintained.

If you don't have all the right resources in-house, knowledgeable suppliers and consultants can help. IEC 61511 is an international standard, its life-cycle model is well understood, and it is being applied by a large number of companies. As the groundswell for its use continues, the number of knowledgeable resources will also increase — making it ever easier to find qualified assistance.

The PlantWeb Advantage

As the provider of the industry's first smart SIS, Emerson also offers a full range of services to help ensure your safety system provides the protection you need...and keeps providing it. These services – including analysis and design, implementation, maintenance, and modification -- span the full lifecycle of your system, with TÜV-certified compliance to IEC 61511 best practices. If you want, we can also train your staff to make the most of your SIS, or provide access to Emerson field safety engineers in your area for ongoing support and maintenance.

Benefits of Complying

Depending on where you're located, compliance with IEC 61511 or other safety standards may be a legal requirement. Even if it's not, doing so makes good sense.

For one thing, the committee that developed IEC 61511 included globally recognized safety experts who drew on their their combined knowledge and experience to create the standard. The result is a rigorous set of "best practices" for engineering, implementing, verifying, operating, and maintaining robust and reliable safety instrumented systems.

In short, it's a good way to help ensure the safety of your plant and community, while also minimizing lifecycle costs.

But even when safety incidents do occur, having complied with the standard can help.

Agencies endorsing IEC 61511 include

Factory Mutual Insurance Company

U.S. Occupational Health and Safety Administration (OSHA)

U.S. Environmental Protection Agency (EPA)

Automation, Software and Information Technology ASI of TÜV Industrial Services GmbH

United Kingdom's Health & Safety Executive (HSE)

Investigations that follow an accident or environmental release often involve government agencies that have the authority to levy fines, send people to jail, close down a facility — or all three. Among the questions they're likely to ask are

- Has this sort of incident occurred within this company or facility previously?
- What proactive processes were used to identify risks?
- What methods were used to quantify risks?
- What actions were taken to mitigate risks?
- What process was followed to ensure the mitigation was properly deployed?
- What processes are in place to ensure the mitigation solution continues to perform as expected over time?

Answers to those sorts of questions are exactly what is produced by using IEC 61511. You may still face a tough investigation, but if you can prove that conformance to the IEC safety standard was appropriately defined, achieved, and maintained, you'll also reduce the risk of the investigating agency's sending anyone to jail or closing down the plant.

Summary

In this course you've learned that:

- For the process industries, key safety standards are IEC 61508, IEC 61511, and ANSI/ISA S84.00.01-2004.
- Today, in the process industries IEC 61511 or the new S84 is the best choice for end-users implementing a safety project or operating and maintaining a safety system.
- All three standards use a performance-based life-cycle model, which makes it easier to integrate them with other standards — and to produce high-quality results at the least possible cost.
- IEC 61511 allows you some freedom to customize the life-cycle model to meet your needs, as long as you meet the standard's requirements. Doing so requires providing adequate funding, people, and training.
- Besides helping you keep your plant, personnel, and community safe, standards compliance can make it easier to deal with investigations after a safety incident.