

FAQ SHEET

S84 / IEC 61511 STANDARD FOR SAFETY INSTRUMENTED SYSTEMS

Acronyms and Abbreviations Used

ANSI	-	American National Standards Institute
BPCS	-	Basic Process Control System
E/E/PES	-	Electrical / Electronic / Programmable Electronic Systems
ESD	-	Emergency Shutdown System
IEC	-	International Electrotechnical Commission
IPL	-	Independent Protection Layer
ISA	-	Instrumentation Society of America (now called The Instrumentation, Systems and Automation Society)
LOPA	-	Layers of Protection Analysis
PES	-	Programmable Electronic System
PFDD	-	Probability of Failure on Demand
SIL	-	Safety Integrity Level
SIS	-	Safety Instrumented System
SRS	-	Safety Requirements Specifications

What is S84 / IEC 61511?

It is a US and international industry standard (ANSI/ISA S84.00.01-2004 / IEC 61511, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, called S84 / IEC 61511 herein). Its objective is to define requirements for Safety Instrumented Systems (SISs) and Safety Instrumented Functions (SIFs).

What are SISs?

SISs take the process to a safe state when predetermined conditions are violated, such as set points for pressure, temperature, level, etc. In other words, they trip the process when they detect an out-of-limit condition. Other terms commonly used for SIS include Emergency Shutdown System (ESD, ESS), Safety Shutdown System (SSD), and Safety Interlock System (SIS). These systems are often automated but can also involve human action in response to alarms.

What are SIFs?

SIFs are actions taken by a SIS to bring the process or equipment under control to a safe state. Each SIF consists of a set of actions to protect against a single specific hazard. One or more SIFs may be implemented in a SIS for a common purpose, e.g. protection of the same process. For example a SIS designed to protect a process may contain three SIFs: high reactor temperature closes the two reactor feed valves, high column temperature or high column pressure closes a reboiler steam valve, high column pressure closes the two reactor feed valves.

Why was S84 / IEC 61511 developed?

S84 / IEC 61511 is based on international standards from the International Electrotechnical Commission (IEC). A performance-based umbrella standard applies to any industrial process that uses E/E/PES (IEC 61508, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, Parts 1 - 7, 1998 - 2000). It is intended to allow the development of industry-specific standards.

A process-sector specific version of IEC 61508 has been developed (IEC 61511, Functional Safety -Safety Instrumented Systems for the Process Industry Sector, Parts 1 - 3, 2003 - 2004).

When does S84 / IEC 61511 apply?

It applies when functional safety is achieved using one or more SIFs in a SIS for the protection of personnel, public or the environment. It may be applied to non-safety issues, e.g. asset protection. S84 / IEC 61511 covers a wide variety of process sector industries including chemicals, oil refining, oil and gas production, pulp and paper, and nonnuclear power generation.

Can you tell me more about SIS?

SISs provide safety control functions and complement the Basic Process Control System (BPCS) which provides normal process control. Ideally, SISs and the BPCS should be independent. SISs provide a layer of protection to help protect the process against accidents.

SISs are composed of:

- Sensors
- Logic solvers
- Power supplies
- Field wiring
- Final control elements
- Communications interfaces

They may include hardware, software and humans. Examples of sensors are pressure and level transmitters. An example of a final control element is an emergency block valve. Logic solvers addressed by S84 / IEC 61511 are primarily Electrical / Electronic / Programmable Electronic Systems (E/E/PES). However, the basic principles of the standard should be applied for other types of logic solvers, such as pneumatic or hydraulic. S84 / IEC 61511 applies to SIS sensors and final control elements regardless of the technology used.

Communications interfaces include human interfaces with the process such as operator interaction with the SIS through video displays and mechanic interaction during maintenance of the SIS as well as internal communications within and between SIS.

How do SIS relate to other layers of protection?

Process designers use a variety of protection layers, or safeguards, to provide a defense in depth against catastrophic accidents. They are devices, systems or actions that are capable of preventing a scenario from proceeding to an undesired consequence. For example, they may be:

- Inherently safe design features
- Physical protection such as relief devices
- Post-release physical protection such as fire suppression systems
- Plant and community emergency response
- SIS

Ideally such protection layers should be independent from one another so that any one will perform its function regardless of the action or failure of any other protection layer or the initiating event. When they meet this criterion they are called Independent Protection Layers (IPL). Not all safeguards meet the independence requirements to be classified as an IPL, although all IPLs are safeguards. For example, two standby pumps that are both electrically powered do not fail independently in the event of loss of power.

Do I always need SIS?

The philosophy of S84 / IEC 61511 is that SIS should be installed only if other non-instrumented systems cannot adequately mitigate process risk. Therefore, an evaluation must be made to determine if an adequate number of non-SIS protection layers has been provided for a process. The method for doing so is not specified by S84 / IEC 61511. However, Layers of Protection Analysis (LOPA) is commonly used and is one of several methods described in S84 / IEC 61511.

How do you account for the varying effectiveness of protection layers?

The effectiveness of an IPL is described in terms of the probability it will fail to perform its required function when called upon to do so (a demand), and the scenario continues towards the undesired consequence despite the presence of the IPL. This is called the *probability of failure on demand (PFD)*. In the case of SIFs the PFD is described and categorized by a Safety Integrity Level (SIL).

Can you tell me more about SIL's?

Once the need for a SIS/SIFs has been identified, the key is to determine the required SIL to control process risk to a tolerable level. The SIL is used as a performance measure (in terms of the probability of the SIF failing to perform its required function on demand).

Four discrete integrity levels are defined in S84 / IEC 61511 (SIL 1, SIL 2, SIL 3, SIL 4). The higher the SIL level, the higher the availability of the SIS. SIL's are defined in terms of PFD:

SIL LEVEL	PFD (Probability of Failure on Demand)
1	0.1 to 0.01
2	0.01 to 0.001
3	0.001 to 0.0001

Techniques such as LOPA are used to determine the required SIL for a SIF in a SIS.

What does S84 / IEC 61511 require?

S84 / IEC 61511 applies a Safety Life Cycle approach and addresses SIS from conceptual design to decommissioning, i.e. cradle to grave.

S84 / IEC 61511 addresses:

- Management of functional safety
- Safety life-cycle requirements
- Verification
- Process hazard and risk assessment
- Allocation of safety functions to protection layers
- SIS safety requirements specification
- SIS design and engineering
- Requirements for application software, including selection criteria for utility software
- Factory acceptance testing
- SIS installation and commissioning
- SIS safety validation
- SIS operation and maintenance
- SIS modification
- SIS decommissioning
- Information and documentation requirements

Can you summarize what S84 / IEC 61511 does and doesn't do?

There are three issues for SIS:

- Are they needed?
- What type should be provided?
- What design should be used and how can its integrity be maintained throughout its life?

Techniques such as LOPA address the first issue. However, they do not determine the types of SIS to provide. They can help choose between alternatives.

The second issue on selecting the type of SIS to install is the province of the process designer and the control systems engineer.

S84 / IEC 61511 does address the third issue. It provides requirements for SIS.

Why should I comply with S84 / IEC 61511?

First, S84 / IEC 61511 represents best practice.

Second, OSHA has endorsed S84 / IEC 61511 as a “national consensus standard” for the application of safety instrumented systems for the process industries (March 23, 2000 OSHA letter to L. M. Ferson, ISA). This letter states that ANSI/ISA S84 / IEC 61511.01-1996 (the first edition of S84 / IEC 61511) is considered “a recognized and generally accepted good engineering practice” for SIS.

Note that Paragraph (d)(3)(ii) of OSHA’s PSM standard, CFR 1910.119, specifies: “The employer shall document that equipment complies with recognized and generally accepted good engineering practices”. The letter states that in evaluating whether an employer's engineering practices with respect to SIS comply with PSM, OSHA would consider, among other factors, whether the employer meets the requirements of S84 / IEC 61511.

In the letter OSHA states that it is also important to note that there is a large percentage of processes which are not covered by PSM which may include SIS covered by S84 / IEC 61511. OSHA states that the employer may be in violation of the General Duty Clause, Section 5(a)(1) of the OSH Act if SIS are utilized which do not conform with S84 / IEC 61511, and hazards exist related to the SIS which could seriously harm employees.

Consequently, this means that OSHA requires companies to comply with S84 / IEC 61511, not only for PSM-covered processes but also for other processes that use SIS where hazards to personnel may be present.

How can I get more information?

Contact Primatech at:

50 Northwoods Blvd.
Columbus, OH 43235
Tel 614-841-9800
Fax 614-841-9805
www.primatech.com

About Primatech

Primatech specializes in Process Safety, Security and Risk Management. We offer consulting, training and software to assist our clients in identifying and reducing the risks posed by toxic, flammable, and explosive materials.

Companies in a variety of industries choose Primatech to help them manage the risks posed by such hazardous materials. We help companies reduce the likelihood and consequences of releases, which helps protect employees and the public and prevent damage to equipment and the environment. Reducing these risks also improves productivity and quality. We help companies comply with OSHA's Process Safety Management (PSM) standard, EPA's Risk Management Program (RMP) regulation, and industry guidelines.

Our capabilities include:

- **Process Hazard Analysis (PHA)**
- **Compliance Audits and Program Assessments**
- **PSM Program Development and Implementation**
- **RMP Program Development and Implementation**
- **Release and Spill Assessment**
- **Process Security Management**
- **Threat and Vulnerability Analysis for Deliberate Acts Including Terrorism**
- **S84 - Safety Instrumented Systems**
- **Layers of Protection Analysis (LOPA)**
- **Operating and Maintenance Procedures Development**
- **Mechanical Integrity Program Development and Implementation Guidance**
- **Human Factors and Human Error Analysis**
- **Facility Siting Analysis**
- **Dispersion and Consequence Modeling**
- **Probability Modeling**
- **Quantitative Risk Assessment**
- **Emergency Response Program Development and Implementation Guidance**
- **Expert Witness Testimony and Litigation Support**

Primatech's clients are often Fortune 500 companies but also include medium and smaller sized companies. We specialize in serving the process industries, and have served hundreds of industrial facilities throughout the world.

- Aerospace
- Agricultural chemicals
- Ammonia facilities
- Bulk/commodity chemicals
- Chlorine facilities
- Cold storage warehousing
- Electronics manufacturing
- Food processing
- Hazardous waste treatment
- Inorganic chemicals
- Mining
- Municipal water treatment
- Oil and gas production and distribution
- Oil and gas pipelines and terminals
- Organic chemicals
- Paints, coatings, resins and adhesives
- Petrochemicals
- Petroleum refining
- Pharmaceuticals
- Polymers and resins
- Propane storage and distribution
- Pulp and paper
- Rubber and plastics
- Semiconductors
- Specialty metals
- Steel
- Water treatment
- Wastewater treatment

Our services and products enable our clients to achieve their risk, safety and security objectives faster and easier. Primatech is an independent company with no vested interests and is seen, therefore, to deliver work recognized as objective and unbiased.